



USSTRATCOM



Global Innovation and Strategy Center

Collaborating with the Private Sector

Summer 2009 – Project 09-03

August 2009



Intern Researchers:

Frederick Bartell
Carrie Lacy
Melissa Moraczewski
Tanya Nodlinski
Sarah Norris
Kate Prasse
Ashley Thomalla
Katherine Zielinski

Project Management and Oversight:

John G. Hudson II, Ph.D.
Sarah Mussoni, M.Ed
Nicholas Arreola
June Edwards, Esq.

Outreach Contributor:

CIC Aaron Brugman

Approved: Tom Gilbert, Col, USAF
Director, Global Innovation and Strategy Center

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

This is not the opinion of USSTRATCOM or the Department of Defense.
This is an informative report to document intern research.

REPORT DOCUMENTATION PAGE					<i>Form Approved OMB No. 0704-0188</i>	
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.						
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.						
1. REPORT DATE (DD-MM-YYYY) AUGUST 2009		2. REPORT TYPE FINAL REPORT			3. DATES COVERED (From - To) MAY 2009 - AUGUST 2009	
4. TITLE AND SUBTITLE Collaborating with the Private Sector					5a. CONTRACT NUMBER N/A	
					5b. GRANT NUMBER N/A	
					5c. PROGRAM ELEMENT NUMBER N/A	
					5d. PROJECT NUMBER 09-03	
6. AUTHOR(S) Frederick Bartell, Carrie Lacy, Melissa Moraczewski, Tanya Nodlinski, Sarah Norris, Kate Prasse, Ashley Thomalla, Katherine Zielinski					5e. TASK NUMBER	
					5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) USSTRATCOM Global Innovation and Strategy Center (GISC) Intern Program 6805 Pine Street Omaha, NE 68106					8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) USSTRATCOM Global Innovation and Strategy Center (GISC) 6805 Pine Street Omaha, NE 68106					10. SPONSOR/MONITOR'S ACRONYM(S) USSTRATCOM - GISC	
					11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.						
13. SUPPLEMENTARY NOTES						
14. ABSTRACT Attacks on the nation's networks are increasing exponentially, as is a growing dependency on cyberspace. It is imperative that the nation's critical infrastructure is protected, especially telecommunications, financial systems, the water supply, electrical grids, and transportation. Currently, the private industry owns 85 percent of the nation's critical infrastructure, while the U.S. government owns only 15 percent. Thus, the U.S. government must work with the private industry to create a collaboration that will protect and defend cyberspace. Many experts emphasize the need to secure the nation's cyber domain, but also acknowledge that actually doing so will probably not occur until there is a cyber disaster, such as a cyber 9/11. The report focuses on discussing the legal barriers to collaboration between the U.S. government and the private sector. Initially, a list of over 30 bodies of law pertaining to cyberspace were compiled, but the focus was narrowed to include only those dealing specifically with collaboration. Non-legal barriers that hinder collaboration, including information-sharing, data classification, and differing motivations and culture are also addressed.						
15. SUBJECT TERMS Cyber law, cyberspace, critical infrastructure, legal barriers, collaboration, information-sharing, classification, business, training, private sector, laws, Patriot Act, FISA, FAR, Intellectual Property, Antitrust Law, Title 10, Title 50, FOIA, FACA, data classification, culture, education, legal, non-legal barriers, e-threats, cyber domain, partnering, private industry						
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 111	19a. NAME OF RESPONSIBLE PERSON Dr. John G. Hudson II	
a. REPORT U	b. ABSTRACT U	c. THIS PAGE U			19b. TELEPHONE NUMBER (Include area code) 402-398-8034	

For additional information or questions concerning this report, please contact the following individuals:

Intern Program Manager:

John G. Hudson II, Ph.D., YA-02, DAF

Commercial (402) 398-8034

John.Hudson@thegisc.org

John.Hudson@stratcom.mil

Intern Program Administration:

Sarah Mussoni, M.Ed, YA-02, DAF

Commercial (402) 398-8028

Sarah.Mussoni@thegisc.org

Sarah.Mussoni@stratcom.mil

GISC Innovation Division Chief:

Ms. Elizabeth Durham-Ruiz, YF-03, DAF

Commercial (402) 398-8022

elizabeth.durhamruiz@thegisc.org

Durhame@stratcom.mil

GISC Innovation Deputy Division Chief:

Mr. Ron Moranville, YA-02, DAF

Commercial (402) 398-8021

ron.moranville@thegisc.org

Moranvil@stratcom.mil

TABLE OF CONTENTS

TABLE OF CONTENTS	II
FIGURES	V
ACRONYMS	VI
PREFACE	VII
EXECUTIVE SUMMARY	VIII
INTRODUCTION	1
DEFINITIONS	7
Collaborate	7
Critical infrastructure	7
Critical Infrastructure Protection.	7
Cyberspace	7
Defend.....	8
E-Threats	8
Private Sector.....	8
Protect	8
THE USA-PATRIOT ACT	9
Overview	9
Application	11
FISA	13
Overview	13
Application	17
GOVERNMENT CONTRACTS UNDER THE FEDERAL ACQUISITIONS REQUIREMENTS.....	21
Overview	21
Application	22
DOD AUTHORITIES.....	25
Title 10.....	25
Overview	25
Application	26
Posse Comitatus Act.....	28
Overview	28

Application	29
Title 50.....	30
Overview	30
Application	32
LAWS AFFECTING BUSINESS PROPERTY AND COMPETITION	33
Intellectual Property.....	33
Patents & Trade Secrets.....	33
Overview	33
Application	35
Trademarks	36
Overview	36
Application	37
Copyrights	37
Overview	37
Application	38
Antitrust: The Sherman Act.....	39
Overview	39
Application	43
PUBLIC ACCESS TO GOVERNMENT INFORMATION	46
FOIA	46
Overview	46
Exemptions.....	47
Application	54
FACA.....	55
Overview	55
Exemptions.....	57
Application	58
NON-LEGAL BARRIERS	59
Information-Sharing	59
Classification Issues.....	60
CULTURE	62

Differing Motivations.....	62
Additional Cultural Issues.....	63
Citizenship Issues	63
Speed of Decision-Making Cycle	64
Consequences of Information Leaks.....	64
Evaluating Cyber Threats.....	65
User Culture	65
LEGAL RECOMMENDATIONS.....	68
FISA	68
FOIA	70
Antitrust.....	70
NON-LEGAL RECOMMENDATIONS.....	73
Develop a Common Language	73
Decrease Over-Classification.....	73
Change Security Clearance Protocol	74
Begin Collaboration with Bilateral Agreements	74
Shift Culture through Training and Education.....	75
Shifting Business and Government Culture through Training	75
Shifting User Culture through Education	76
ISHARE – A NEW APPROACH TO PARTNERING	77
ISHARE AS A NON-PROFIT ENTITY	80
ISHARE and Legal and Non-Legal Barriers.....	81
Legal.....	81
Non-Legal	83
FUTURE RESEARCH.....	84
CONCLUSION	89
BIBLIOGRAPHY	90
APPENDIX 1: OUTREACH CONTRIBUTORS.....	97
APPENDIX 2: ABOUT THE AUTHORS.....	100

FIGURES

Figure 1: Distribution of Critical Infrastructure.....	2
Figure 2: Initial Legal Considerations.....	3
Figure 3: Legal Research Methodology.....	4
Figure 4: The Real Issues are Non-Legal	61
Figure 5: Summary of Differences Between Existing Programs and ISHARE.....	81

ACRONYMS

ACLU	American Civil Liberties Union
CBI	Confidential Business Information
CERT	Computer Emergency Response Teams
CII	Critical Infrastructure Information
CIP	Critical Infrastructure Protection
D.A.R.E.	Drug Abuse Resistance Education
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DoD	Department of Defense
DoJ	Department of Justice
FACA	Federal Advisory Committee Act
FAR	Federal Acquisitions Regulations
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FTC	Federal Trade Commission
G8	Group of Eight
GAO	Government Accountability Office
HSPD-7	Homeland Security Presidential Directive-7
I3P	Institute for Information Infrastructure Protection
INTERPOL	International Police
IP	Internet Protocol
ISAC	Information Sharing and Analysis Centers
ISHARE	Information Sharing to Help America Recognize and Respond to E-Threats
IT	Information Technology
LAA	Limited Access Authorizations
NATO	North Atlantic Treaty Organization
NRP	National Response Plan
NSA	National Security Agency
OAS	Organization of American States
PCA	Posse Comitatus Act
USA-PATRIOT	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism
UN	United Nations
USG	United States Government
WTO	World Trade Organization

PREFACE

This report is the product of the Global Innovation and Strategy Center's (GISC) Internship program. The original request for this project was submitted by U.S. Strategic Command (USSTRATCOM). The internship program consists of teams of graduate and undergraduate students who work on semester-long projects with the goal of providing a multidisciplinary, unclassified, non-military perspective on important Department of Defense (DoD) issues.

The summer 2009 team, composed of nine students from Creighton University, the University of Nebraska at Omaha, the University of Nebraska at Lincoln, and the United States Air Force Academy was tasked with determining the legal and non-legal barriers that need to be addressed if the DoD collaborates with the private sector to protect and defend cyberspace. While the GISC provided the resources and technology for the project, it was solely up to the team to develop the project design, conduct the research and analysis, and provide appropriate recommendations.

The team was allotted 90 days to research, conduct outreach to experts in a variety of fields, brief the customer, and write the final report. A variety of professional, academic, government, and private sector experts provided information, generated answers for the project question, and posed additional questions to consider when working toward achieving the project objective.

The team is grateful for the contributions of the many experts interviewed during outreach. Much credit belongs to the expert interviewees who contributed their time and knowledge. (See Appendix A for a full list of outreach contributors.)

EXECUTIVE SUMMARY

Attacks on the nation's networks are increasing exponentially, as is a growing dependency on cyberspace. It is imperative that the nation's critical infrastructure be protected, especially telecommunications, financial systems, the water supply, electrical grids, and transportation. Currently, the private industry owns 85 % of the nation's critical infrastructure, while the government owns only 15 %. Thus, the government must work with the private industry to create a collaboration that will protect and defend cyberspace. Many experts emphasized the need to secure the nation's cyber domain, but also acknowledged that actually doing so will probably not occur until there is a cyber disaster, such as a "Cyber 9/11." The team was allotted 90 days to conduct open-source research, write a comprehensive report, and provide an executive briefing to the U.S. Strategic Command Commander and Staff, U.S. government agencies, and other interested parties. The project focused on discussing the legal barriers to collaboration between the U.S. government and private sector. Initially, the team compiled a list of over 30 bodies of law pertaining to cyberspace, but narrowed the focus to include only those dealing specifically with collaboration. Extensive outreach efforts left the team with the following list of laws:

- USA-PATRIOT Act (Patriot Act)
- Foreign Intelligence Surveillance Act (FISA)
- Federal Acquisition Regulation (FAR)
- Intellectual Property
- Antitrust Law
- Title 10 & Title 50
- Freedom of Information Act (FOIA)

- Federal Advisory Committee Act (FACA)

Non-legal barriers that hinder collaboration also arose while talking to experts, including information-sharing concerns, classification of data, and differing motivations and culture. The team proposed six strategies to address barriers to collaboration:

- Enact FISA amendment and construct FOIA amendment for information-sharing
- Develop an exemption for information-sharing under Antitrust Law
- Decrease over-classification of information
- Begin collaboration with bi-lateral agreements
- Shift user culture through education and training
- Establish a more collaborative non-profit organization with shared authorities and responsibilities across the private sector and government

INTRODUCTION

U.S. cyber networks are constantly attacked. Network attacks affect both the private sector and the government. For example, in 2008 a Fortune 500 company reported that 285 million records were compromised, meaning the information contained was leaked, stolen, made public, or endangered in some way.¹ This number of compromised records from a single corporation exceeded the total number of breached records from 2004 to 2007 combined.² A report issued by the same company stated that compromised sensitive information and security breaches are a major concern worldwide for organizations.³ That company's report emphasized the need to rapidly respond when such a breach is discovered. Network attacks are also a problem for the Department of Defense (DoD), which operates and manages 15,000 of its own networks.⁴ According to an article in Government Technology, a non-DoD actor attempts to gain unauthorized access to these networks every six seconds.⁵

Additionally, the nation's critical infrastructure relies on cyber networks for conducting operations. The definition of critical infrastructure is continuously evolving with many working definitions used by government agencies. For purposes of this report, the team has defined critical infrastructure as the physical and virtual networks and systems that provide essential resources necessary to maintain and operate the economy, government, and society at large. Such critical infrastructure includes, but is not limited to, electrical power systems, telecommunications, financial services, gas and oil, water, transportation, and emergency

¹ Baker, Wade H., et al. "2009 Data Breach Investigations Report." Verizon Business. 17 Aug. 2009 <http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf>.

² Baker, Wade H., et al.

³ Baker, Wade H., et al.

⁴ "Smart Card Alliance Government Conference Opens with DOD Network Security Case Study." Government Technology: Solutions for State and Local Government in the Information Age. 19 Jun. 2009 <<http://www.govtech.com/gt/articles/104934>>.

⁵ "Smart Card Alliance Government Conference Opens with DOD Network Security Case Study."

services. Figure 1 is a graphical representation of the distribution of critical infrastructure across the public and private sectors. According to a report issued by the United States Government Accountability Office (GAO), the private sector owns 85 % of the nation's critical infrastructure, whereas the government owns 15 %.⁶ Because the government owns such a small percentage, collaboration between the private sector and the government is imperative to secure the vast amount of information held in cyberspace.⁷

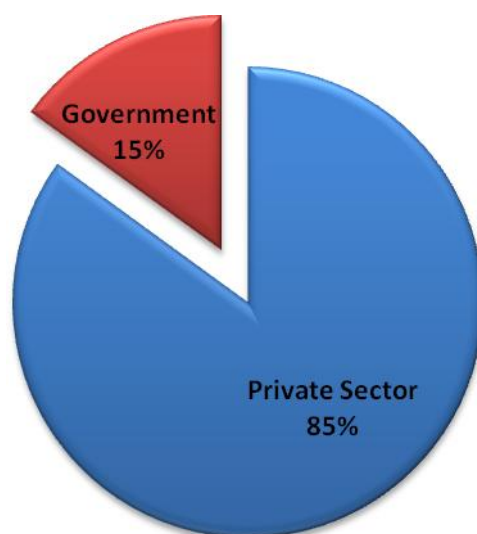


Figure 1: Distribution of Critical Infrastructure

⁶ "Critical Infrastructure Protection." GAO Highlights. 7 June 2009 <<http://www.gao.gov/highlights/d0739high.pdf>>.

⁷ "Critical Infrastructure Protection." GAO Highlights. 7 June 2009 <<http://www.gao.gov/highlights/d0739high.pdf>>.

Because of the broad reach of cyber in the U.S. society, the team began the project with a period of independent research focused on potential legal barriers. Figure 2 depicts the potential legal barriers identified by the team prior to conducting outreach efforts.

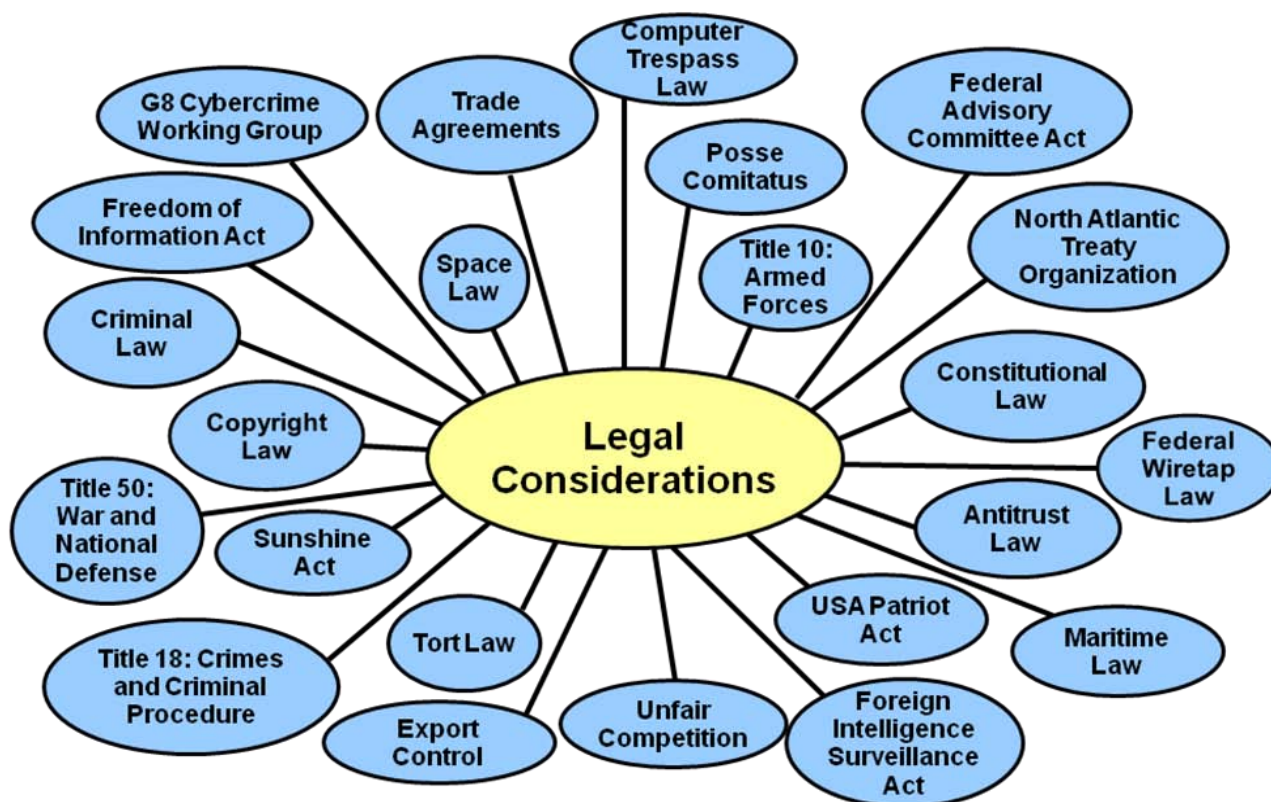


Figure 2: Initial Legal Considerations

After conducting outreach with representatives from the government, industry, and academia, the team narrowed the scope of the project to focus solely on those legal considerations that were collaboration barriers. This resulted in a significantly smaller list of laws to consider. If the private sector perceived a law was a barrier, the team viewed it as a barrier. Since the goal of the project was to encourage collaboration, any perceived barriers would need to be addressed, regardless of whether or not the law actually presented a barrier.

In conducting outreach with private industry, the team requested to speak with company representatives who could discuss the legal issues that presented barriers for collaboration. However, the team most frequently had the opportunity to discuss these issues with information security and technology, public relations, and policy representatives. The private industry outreach interviewees were rarely, if ever, represented by their legal departments. Accordingly, the interviews were informed by the experiences and input from individuals in a non-legal capacity. This could be a sign of the private sector's hesitancy to discuss the legal aspects of this issue, or it could be indicative of the fact that the private sector does not prioritize legal aspects for cyber collaboration. Regardless, the input from the interviewees still touched on several legal issues. Figure 3 depicts the team's legal-specific research methodology.

	Pertains to Collaboration	Emphasized in Outreach	Cited as Significant	Where Addressed
Antitrust Law	✓	✓	✓	Brief and Research Paper
Constitutional Law	✓	✓	✓	Brief and Research Paper
Federal Advisory Committee Act	✓	✓	✓	Brief and Research Paper
Federal Acquisition Regulation	✓	✗	✗	Research Paper
Foreign Intelligence Surveillance Act	✓	✓	✓	Brief and Research Paper
Freedom of Information Act	✓	✓	✓	Brief and Research Paper
Intellectual Property	✓	✓	✗	Research Paper
USA Patriot Act	✓	✓	✗	Research Paper
Posse Comitatus Act	✓	✗	✗	Research Paper
Sunshine Act	✓	✗	✗	Research Paper
Unfair Competition	✓	✗	✗	Research Paper



 Yes
 No

Figure 3: Legal Research Methodology

The first column on the chart represents the 11 laws that pertain in some manner to collaboration. The second column represents which of these laws were most often identified by outreach experts as germane to collaboration. The third column indicates laws cited in outreach as significantly impacting collaboration. The fourth column shows in what capacity each law was discussed during the research capacity: in the executive briefing provided to the U.S. Strategic Commander and customers, the comprehensive report, or both. This report discusses the laws listed in Figure 3 and further elaborates upon those which were cited as significant. The discussion of each law will include its background, meaning, and impact on efforts to collaborate.

Upon completion of the legal discussion, the analysis of the problem will shift focus to non-legal considerations. The extensive outreach efforts led to the conclusion that the most significant barriers to collaboration are non-legal. Discussion of non-legal considerations includes trust issues between the private sector and government, information-sharing concerns, classification of data and the security clearance process, differing motivations of each sector, and cultural concerns among collaborating parties.

Finally, recommendations to address barriers to collaboration will include both legal and non-legal considerations. The legal recommendations include proposed amendments to laws cited as perceived or actual barriers to collaboration, which include the Foreign Intelligence Surveillance Act (FISA), the Freedom of Information Act (FOIA), Antitrust Law, and the Federal Advisory Committee Act (FACA). The non-legal recommendations include decreasing over-classification, beginning collaboration efforts with small bi-lateral agreements, reassessing security clearance protocol, and an overall shift in culture. Finally, the team recommends the creation of a non-profit organization called Information Sharing to Help America React and Respond to E-threats,

or ISHARE, as an information-sharing mechanism. ISHARE could remedy many of the real and perceived barriers to collaboration encompassing many of the team's legal and non-legal recommendations.

DEFINITIONS

In order to provide a comprehensive understanding of the team's research, findings, and final recommendations, the following standard definitions will be used in this report.

- ***Collaborate***: to share information [on cyber threats and vulnerabilities] and to “work together, esp. in a joint intellectual effort.”⁸
- ***Critical infrastructure***: “The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole.”⁹ The “physical and cyber-based systems essential to the minimum operations of the economy and government.”¹⁰
- ***Critical Infrastructure Protection***: “Actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets.”
Depending on the risk, these actions could include: changes in tactics, techniques, or procedures; adding redundancy; selection of another asset; isolation or hardening; guarding; and etc.¹¹
- ***Cyberspace***: “A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet,

⁸ “Collaborate.” Webster’s II New Riverside University Dictionary. 1984

⁹ “Executive Order 13010 - Critical Infrastructure Protection.” Federal Register. 13 Aug. 2009
<<http://www.fas.org/irp/offdocs/eo13010.htm>>.

¹⁰ “The Clinton Administration’s Policy on Critical Infrastructure Protection: Presidential Decision Directive 63.” Presidential Decision Directives. 17 Aug. 2009 <<http://fas.org/irp/offdocs/paper598.htm>>.

¹¹ “Critical Infrastructure Protection.” DOD Dictionary of Military Terms. 12 Aug. 2009
<<http://www.js.pentagon.mil/doctrine/jel/dict/data/c/11427.html>>.

telecommunications networks, computer systems, and embedded processors and controllers.”¹²

- **Defend:** “To protect from danger, attack, or harm: guard.”¹³
- **E-Threats:** Any type of threat that affects the functionality and security of cyberspace.¹⁴
- **Private Sector:** “An umbrella term that may be applied in the United States and in foreign countries to any or all of the nonpublic or commercial individuals and businesses, specified nonprofit organizations, most of academia and other scholastic institutions, and selected nongovernmental organizations.”¹⁵
- **Protect(ion):** 1. “Preservation of the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area..”¹⁶

¹² “Cyberspace.” DOD Dictionary of Military Terms. 12 Aug. 2009
<<http://www.js.pentagon.mil/doctrine/jel/DODdict/data/c/10160.html>>.

¹³ “Defend.” Webster’s II New Riverside University Dictionary. 1984.

¹⁴ Generated by Research Team.

¹⁵ “Private Sector.” DOD Dictionary of Military Terms. 12 Aug. 2009
<<http://www.js.pentagon.mil/doctrine/jel/DODdict/data/p/19545.html>>.

¹⁶ “Protection.” DOD Dictionary of Military Terms. 12 Aug. 2009
<<http://www.js.pentagon.mil/doctrine/jel/DODdict/data/p/10741.html>>.

THE USA-PATRIOT ACT

Overview

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA-PATRIOT) Act, also known as the Patriot Act, is an anti-crime and anti-terrorist law enacted on October 26, 2001 in response to the September 11, 2001 attacks.¹⁷ Notably, the Patriot Act amended both the Federal Wiretap Act and the Foreign Surveillance Intelligence Act (FISA). The Federal Wiretap Act served to protect the privacy of oral, wire, or electronic communications including web browsing and internet communications such as email.¹⁸ Furthermore, it regulated the interception of electronic communications, which refers to acquiring any electronic communication made through the use of an electronic or mechanical device.¹⁹ The Patriot Act amendments to the Federal Wiretap Act granted extensive powers to specific U.S. government agencies, such as the National Security Agency (NSA), to not only monitor, but to also intercept electronic communications, including those previously protected or restricted by the Federal Wiretap Act.²⁰

FISA was also changed in significant ways by the Patriot Act. Specifically, § 215 of the Patriot Act allows for the Federal Bureau of Investigation (FBI) to have greater search and seizure powers, which were previously restricted under FISA. As will be discussed later in this section, the team's research revealed the Patriot Act's amendments to the Federal Wiretap Act and FISA

¹⁷ Lewis, Neil. "Patriot Act." *Microsoft Encarta Online Encyclopedia 2009*. 7 Jul. 2009 <http://encarta.msn.com/encyclopedia_701712693/Patriot_Act.html>.

¹⁸ "An Overview of the Federal Wiretap Act, Electronic Communications Privacy Act, and State Two-Party Consent Laws of Relevance to the NebuAd System and Other Uses of Internet Traffic Content from ISPs for Behavioral Advertising." *Center for Democracy & Technology*. 14 Aug. 2009 <<http://www.cdt.org/privacy/20080708ISPtraffic.pdf>>.

¹⁹ 18 U.S.C. §§ 2510-2522

²⁰ Hudson, David L., Jr. "Patriot Act." *First Amendment Center*. 8 Jul. 2009 <http://www.firstamendmentcenter.org/speech/libraries/topic.aspx?topic=patriot_act>.

create obstacles to collaboration. Although these obstacles might not be specific legal barriers, these amendments create cultural barriers that research indicates can be more difficult to overcome.²¹

In the aftermath of the attacks on the World Trade Center and Pentagon, the executive and legislative branches took rapid actions to enact laws to prevent further terroristic acts. The Patriot Act initially received overwhelming support from the Senate and House of Representatives, passing in the House by a vote of 357 to 66, and with only one dissenting vote in the Senate.²² It also received support from the private sector and citizens, primarily because it was assumed that many of the provisions were temporary.²³ Indeed, many of the most controversial provisions were written with sunset provisions, set to expire on 31 December 2005.²⁴ In March of 2006, however, 14 of the original 16 sunset provisions were made permanent.²⁵ This legislative action was much more controversial than the original enactment as many in the public had begun to have concerns about the extent of powers granted to the government to intercept electronic communications. Many American citizens and a number of private sector entities oppose the Patriot Act as a direct infringement on Constitutional rights, particularly the First and Fourth Amendments.²⁶ The First Amendment guarantees U.S. citizens the following five rights: (1) freedom of religion, (2) freedom of speech, (3) freedom of assembly, (4) freedom of association,

²¹ McDermott, Richard and Carla O'Dell. "Overcoming the 'Cultural Barriers' to Sharing Knowledge." American Productivity & Quality Center. 17 Aug. 2009

<http://www.apqc.org/portal/apqc/ksn/Overcoming%20Cultural%20Barriers.pdf?paf_gear_id=contentgearhome&paf_dm=full&pageselect=contentitem&docid=106967>.

²² Lewis, Neil. "Patriot Act." Microsoft Encarta Online Encyclopedia 2009. 7 Jul. 2009

<http://encarta.msn.com/encyclopedia_701712693/Patriot_Act.html>.

²³ Giacomello, Giampiero. National Governments and Control of the Internet: A Digital Challenge. New York: Routledge, 2005.

²⁴ Doyle, Charles. "USA PATRIOT Act Sunset: A Sketch." CRS Report for Congress. 18 Aug. 2009

<<http://www.fas.org/irp/crs/RS21704.pdf>>.

²⁵ Lewis, Neil.

²⁶ Hudson, David L., Jr. "Patriot Act." First Amendment Center. 8 Jul. 2009

<http://www.firstamendmentcenter.org/speech/libraries/topic.aspx?topic=patriot_act>.

and (5) freedom of press.²⁷ The Fourth Amendment guarantees U.S. citizens the freedom from “unreasonable” search and seizures.²⁸ It also ensures that individuals cannot come under search without a warrant certifying probable cause.²⁹

Some allege that the Patriot Act amendment of the Federal Wiretap Act violates the freedoms of speech and press by allowing the FBI to launch investigations on U.S. citizens “based on opinions they choose to publish, write, or speak, even when done privately through electronic means.”³⁰ Critics view the Patriot Act as conflicting with the freedom from unreasonable search and seizure by allowing foreign intelligence searches for criminal purposes without probable cause of a crime. Robert Levy of the Cato Institute wrote that “the Patriot Act represents the looming sacrifice of civil liberties at the altar of national security.”³¹ Other groups and individuals defined the Patriot Act as a necessary tool for the government to counter the possibility of further terrorist attacks in the Homeland and point to the lack of such attacks as proof that it remains important in protecting the Homeland.

Application

Many interviewees from the private sector stated that the Patriot Act, especially its amendment of the Federal Wiretap Act, has a strong hindering effect on collaboration. However, it is not the law itself that poses a barrier to collaboration, but rather the perceptions of the law and controversy surrounding it among the private sector and American citizens.³² The team’s

²⁷ U.S. Const. amend. I.

²⁸ U.S. Const. amend. IV.

²⁹ “The PATRIOT Act’s Impact on your Rights.” American Civil Liberties Union. 14 Aug. 2009 <<http://www.aclu.org/PatriotActFlash/PatriotActFeature.htm>>.

³⁰ “The Patriot Act and the First Amendment: A Statement from the Freedom to Read Committee of the Association of American Publishers.” 17 Aug. 2009 <<http://www.publishers.org/main/AboutAAP/attachments/patriotact.pdf>>.

³¹ Hudson, David L., Jr. “Patriot Act.” First Amendment Center. 8 Jul. 2009

<http://www.firstamendmentcenter.org/speech/libraries/topic.aspx?topic=patriot_act>.

³² Schlansker, Bob. Personal Interview. 15 Jun. 2009.

research and extensive outreach with members of the private sector and the government often indicated that the Patriot Act created an atmosphere of suspicion and skepticism among members of the private sector and U.S. citizens alike.³³

Particularly, the much publicized 2007 National Security Agency (NSA) AT&T wiretapping conducted under the protection of the Patriot Act amendments contributed to the public's awareness of Title II, Enhanced Surveillance Procedures, under which the warrantless wiretapping was made legal.³⁴ The American Civil Liberties Union (ACLU) promptly challenged this section of the Act in *ACLU v. NSA* in 2007.³⁵ The U.S. Sixth Circuit Court of Appeals dismissed the filing, commenting not on the issue of constitutional infringements, but instead that the ACLU did not have the legal standing to sue because it could not prove that it, nor any other party bringing suit, had fallen victim to the clandestine wiretapping.³⁶ Because of the procedural nature of this ruling, courts have yet to decide whether the expansion of the electronic surveillance power under the Patriot Act violates the Constitution. The current lack of consensus on the legality and necessity of the expansion of the government's ability to intercept electronic communications presents problems for a government and private sector collaboration. If customers of companies believe the companies are "illegally" providing the government with access to customers' communications, the company may lose those individuals as customers.

³³ Topoliski, Robb. Personal Interview. 15 Jun. 2009.

³⁴ "Dispelling the Myths." Department of Justice. 8 Jul. 2009 <http://www.usdoj.gov/archive/ll/subs/u_myths.htm>.

³⁵ "*ACLU v. NSA*." United States Court of Appeals. 14 Aug. 2009 <<http://www.ca6.uscourts.gov/opinions.pdf/07a0253p-06.pdf>>.

³⁶ "*ACLU v. NSA*."

FISA

FISA was mentioned by a majority of outreach experts as being a bar to collaboration with the private sector. However, research reveals that FISA is not an actual legal barrier to collaboration, rather it is the public's concern how FISA will be utilized that inhibits the flow of information-sharing across sectors.

Overview

Congress enacted the original 1978 FISA, 50 U.S.C. § § 1801, et seq. in an effort “to establish checks and balance among the three branches of government” and to curb abuse of warrantless domestic surveillance in the name of national security.³⁷ FISA was a “response both to the Committee to Study Government Operations with Respect to Intelligence Activities (or Church Committee) revelations regarding past abuses of electronic surveillance for national security purposes and to the somewhat uncertain state of the law on the subject.”³⁸ FISA prevents the government from intercepting any international call or email involving individual citizens in the U.S. without a warrant, ensuring U.S. citizen's Fourth Amendment's search and seizure protections are not violated.

FISA permits the President to authorize, through the Attorney General, electronic surveillance without a court order for one year, provided the surveillance is only for foreign intelligence information, is targeting foreign powers, and there is no substantial chance that the surveillance will acquire the contents of any communication to which a U.S. citizen is a party.^{39,40} The

³⁷ U.S. Courts, “Understanding Intelligence Surveillance: A FISA Primer.”

³⁸ Bazan, Elizabeth. “The Foreign Intelligence Surveillance Act: A Sketch of Selected Issues. Congressional Research Service. p. 4. 7 Jul. 2008. 4 Aug. 2009. <<http://www.fas.org/sgp/crs/intel/RL34566.pdf>>.

³⁹ 50 U.S.C. § 1801 (a)(1)-(3)

⁴⁰ 50 U.S.C. § 1802(a)(1)

Attorney General is then required to certify to the Foreign Intelligence Surveillance Court (FISC) that these conditions are satisfied, and to report to the House and Senate intelligence committees.⁴¹ The FISC can grant a warrant if the government establishes probable cause that the target of the surveillance is a foreign power or agent and that the targeted places are being used, or are about to be used, by a foreign power. If a warrant is issued, incidental surveillance of U.S. citizens is authorized. The government official applying for the warrant must ensure the minimization requirements enumerated in § 1804 are met to ensure protection of U.S. citizens.

Since the primary purpose of FISA is to “assist the government, specifically the executive branch, with gathering foreign intelligence, as opposed to evidence of criminal activity,” the FISC is “instructed not to permit surveillance activities if the government’s sole motivation is to use the surveillance for criminal investigative purposes.”⁴² Rather, each application must contain the Attorney General’s certification that the target of the proposed surveillance is either a “foreign power” or “the agent of a foreign power.”⁴³

FISA’s limitations on electronic surveillance only apply when the subject of surveillance is residing within the U.S. Thus, “the government is free to conduct warrantless surveillance operations of individuals so long as those individuals are outside of the borders of the United States.”⁴⁴ Furthermore, “even if an individual is residing in the United States, the President, through the Attorney General, may authorize a warrantless surveillance on the individual for as long as 72 hours if an emergency/necessity dictates.”⁴⁵ However, “the Attorney General must

⁴¹ 50 U.S.C. § 1802 (a)(2)

⁴² U.S. Courts, “Understanding Intelligence Surveillance: A FISA Primer.” 3 Aug. 2009. <<http://www.uscourts.gov/outreach/topics/fisa/whatisfisa.html>>.

⁴³ Federal Judicial History, “Foreign Intelligence Surveillance Court.” 11 Aug. 2009. <http://www.fjc.gov/history/home.nsf/page/fisc_bdy>.

⁴⁴ U.S. Courts.

⁴⁵ U.S. Courts.

inform the FISC as early as possible and it must explain why it was not feasible to first seek the Court's permission before carrying out the surveillance activity.”⁴⁶ In addition, “if Congress declares that a state of war exists, the President, through the Attorney General, may authorize the warrantless surveillance of individuals for as long as 15 days.”⁴⁷

If the government fails to follow these procedural requirements, FISA provides for both criminal and civil sanctions. A member of the government can be subject to criminal sanctions for intentionally engaging in electronic surveillance unless authorized by the statute.⁴⁸ Such an offense is punishable by a fine of no more than \$10,000 and/or imprisonment for five years.⁴⁹ Furthermore, an individual who was the “target of an [illegal] electronic surveillance or any person whose communications or activities were subject to electronic surveillance,” has a cause of action against any person, who committed the FISA violation.^{50,51} This could include a telecommunication (telecom) company that cooperated with the government to allow the surveillance. Recovery includes actual damages, punitive damages, attorney’s fees and litigation costs.⁵² According to the Washington Post, this exact scenario occurred with Qwest Communications International.⁵³

Prior to the 2008 FISA amendments, U.S. citizens could protect their rights against electronic surveillance through a civil lawsuit. The FISA amendments, however, limited the liability of individuals and telecom companies when turning over information or providing access to the

⁴⁶ U.S. Courts, “Understanding Intelligence Surveillance: A FISA Primer.” 3 Aug. 2009.
<<http://www.uscourts.gov/outreach/topics/fisa/whatisfisa.html>>.

⁴⁷ U.S. Courts.

⁴⁸ 50 U.S.C. § 1809 (a).

⁴⁹ 50 U.S.C. § 1809 (c).

⁵⁰ 50 U.S.C. §1801 (k)

⁵¹ 50 U.S.C. §1810.

⁵² 50 U.S.C. §1810 (a)-(c).

⁵³ Nakashima, Ellen and Dan Eggen. “Former CEO Says U.S. Punished Phone Firm.” *Washington Post*. 13 Oct 2007.

government.⁵⁴ Specifically, a civil lawsuit cannot be brought against an electronic communication service provider if the information in question was provided in connection with an intelligence activity involving communications that was authorized by the President between September 11, 2001 and January 17, 2007 and was designed to detect or prevent terrorist activities or attacks against the U.S.⁵⁵

The original FISA also established the Foreign Intelligence Surveillance Court of Review (or Court of Review). The Court of Review evaluates, at the government's request, the denial of a warrant by the FISA Court. According to the Federal Judiciary Center, a research center established by Congress, "Because of the almost perfect record of the Department of Justice in obtaining the surveillance warrants and other powers it requested from the Foreign Intelligence Surveillance Court, the review court had no occasion to meet between 1978 and 2002."⁵⁶

The government's recent success rate in obtaining FISA warrants flows from several FISA amendments, which affected the balance between national security interests and civil liberties.⁵⁷

These amendments have broadened the ability of the government to access information in the name of national security. Whereas the 1978 version of FISA only dealt with electronic surveillance, the Patriot Act amendments to FISA now provide "a statutory framework for gathering foreign intelligence information through the use of electronic surveillance, physical searches, and pen registers or trap and trace devices, and access to business records and other tangible things."⁵⁸ The most recent amendment to the act, the FISA Amendment Act of 2008 extensively broadens the number of targets for electronic surveillance. Prior to the 2008

⁵⁴ 50 U.S.C. § 1885a (a).

⁵⁵ 50 U.S.C. § 1885a (a)(4).

⁵⁶ Federal Judicial History, "Foreign Intelligence Surveillance Court." 11 Aug. 2009. <http://www.fjc.gov/history/home.nsf/page/fisc_bdy>.

⁵⁷ Bazan, Elizabeth. "The Foreign Intelligence Surveillance Act: A Sketch of Selected Issues." Congressional Research Service, p. 4, 7 Jul. 2008. 4 Aug. 2009. <<http://www.fas.org/sgp/crs/intel/RL34566.pdf>>.

⁵⁸ Bazan, Elizabeth.

amendments, FISA prohibited the government from intercepting any international call or email involving individuals in the U.S. without a warrant from the FISA Court based on probable cause. As amended, FISA now permits electronic surveillance without a warrant, even if the target is a U.S. citizen or an individual on U.S. soil, if the surveillance is undertaken for “foreign intelligence” purposes and seeks information about a person reasonably believed to be outside the U.S.⁵⁹

The amended FISA also provides a statutory structure for the installation and use of pen registers and trap and trace devices and for obtaining tangible things necessary for investigation.⁶⁰ In order to obtain tangible items, FISA permits the Director of the FBI or his designee to apply for an order from the FISC. However, the ability of the Attorney General to investigate a U.S. citizen under the amended FISA is limited in that an investigation cannot be conducted solely on the basis of activities protected by the First Amendment to the Constitution.⁶¹ This measure is seen as an attempt to strike a balance between national security needs and First Amendment rights.⁶² Most constitutional law scholars are of the opinion that the 2008 amendments tipped the balance toward the government’s right to investigate and away from individual First and Fourth Amendment rights.⁶³

Application

Of particular interest to this research are the aspects of FISA that affect how the government and cooperating private sector companies interact. Customers provide personal information to

⁵⁹ 50 U.S.C. § 1802 (a).

⁶⁰ 50 U.S.C. § 1841(2) defines “pen register” and “trap and trace device” by cross-reference to 18 U.S.C. § 3127.

⁶¹ 50 U.S.C. § 1842(a)(1); 50 U.S.C. § 1861(a)(1) and (a)(2)(B).

⁶² Bazan, Elizabeth. Congressional Research Service. “The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and U.S. Foreign Intelligence Surveillance Court and U.S. Foreign Intelligence Surveillance Court of Review Decisions.” p. 13. 5 Feb. 2007. 4 Aug. 2009. <<http://www.fas.org/sgp/crs/intel/RL30465.pdf>> ; 50 U.S.C. § 1861(a)(1).

⁶³ Bazan, Elizabeth. “The Foreign Intelligence Surveillance Act: A Sketch of Selected Issues. Congressional Research Service. p. 1. 7 July 2008. 4 Aug. 2009. <<http://www.fas.org/sgp/crs/intel/RL34566.pdf>>.

telecoms, IT companies, or other cyber companies by virtue of the service relationship. Under the amended FISA, the government can use these companies to obtain information on non-U.S. customers when the intercept occurs outside the U.S. This type of surveillance can proceed without a warrant. If the government is acting with a warrant, the intercept may target U.S. citizens and seek communication and records located within the U.S.

While the language of the 2008 amendments limited the liability of those complying with government requests made under FISA, pending litigation brought by customers that challenge the legality of allowing intercepts places that liability limitation in question. The most well-known litigation challenging a telecom's compliance with FISA is *Hepting v. AT&T*, a 2006 class-action lawsuit alleging the telecom violated the law and the privacy of its customers by collaborating with the NSA to wiretap and data-mine Americans' communications.⁶⁴ On June 3, 2009, the presiding judge ruled in favor of the government in dismissing the majority of cases citing the 2008 amendment's limitation of liability. However, an appeal of the order is underway.⁶⁵

Knowing the government has been granted broad power under the amended FISA should encourage companies to turn over information or allow for the use of wiretapping. However, the public has grown suspicious of government surveillance. Private sector outreach participants indicated customers are hesitant to do work with telecoms once it is known the company cooperated with the government and turned over information pursuant to FISA, even if that cooperation is legal. This is because the public has concerns about the actual target of the government's surveillance. Many believe the government is using FISA wiretaps for routine

⁶⁴ "Hepting v. AT&T." Electronic Frontier Foundation. 13 Aug. 2009. < <http://www EFF.org/cases/hepting>>.

⁶⁵ "EFF and ACLU Planning to Appeal Dismissal of Dozens of Spying Cases." Electronic Frontier Foundation. 3 Jun. 2009. 13 Aug. 2009. < <http://www EFF.org/press/archives/2009/06/03>>.

criminal investigations. On the other hand, government interviewees stated that much of the concern about FISA is founded upon misconceptions as the focus is really to obtain information on foreign actors looking to harm the U.S., not to monitor routine communications of U.S. citizens. They also pointed to the fact that many citizens support the expanded intelligence powers. In spite of this, the secretive nature of what the government is actually doing prevents resolution of this debate.⁶⁶ These unanswered concerns affect the ability of the government to effectively work with or collaborate with the private sector.

The public was recently made aware that after September 11, 2001, President George W. Bush authorized the NSA to “eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without the court-approved warrants ordinarily required for domestic spying.”⁶⁷ The Bush administration “maintained that the program was limited to calls from suspected terrorist[s] abroad to an individual inside the U.S.,” but refused to provide records to support this position.⁶⁸ This strengthened concerns that civil liberties were not being prioritized in the name of national security and it further eroded the public’s confidence in the procedural protections under FISA.⁶⁹

Given customer concerns and public perception, the team’s research indicated that FISA does not lower the barrier to collaboration. Rather, the companies interviewed regarded FISA as government compulsion. During outreach, the private sector indicated it has little to gain under FISA other than immunity from lawsuits based on the government’s actions. That is, companies

⁶⁶ Tien, Lee and Peter Eckersley. “Letter to the Administration.” Electronic Frontier Foundation. (undated).

⁶⁷ Risen, James and Eric Lichtblau. “Bush Lets U.S. Spy on Callers Without Courts.” New York Times. 16 Dec. 2005. 13 Aug. 2009.

<<http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=1&ei=5089&en=e32070e08c623ac1&ex=1292389200>>

⁶⁸ Epsley-Jones, Katelyn and Christina Frenzel. “The Church Committee Hearings & The FISA Court.” PBS-Frontline. 15 May 2007. 12 Aug. 2009.

⁶⁹ Risen, James and Eric Lichtblau.

cannot be sued by customers for releasing information to the government or for permitting the government to intercept customer communications and records. But FISA, and the way it has been used by the government, continues to raise customer concerns regarding the privacy of the information provided by their service providers. Since companies cannot opt out of compliance with FISA, companies can do little to ease the concerns of their customers as the company does not determine if or when customers are investigated. FISA, therefore, does not further or encourage collaboration. Rather, FISA creates problems between telecoms and their customers thus affecting these companies' bottom lines. Recommendations to address these concerns appear in the Recommendations section of this report.

GOVERNMENT CONTRACTS UNDER THE FEDERAL ACQUISITIONS REQUIREMENTS

Overview

Outreach experts proposed using the Federal Acquisitions Regulations (FAR) and the government's purchasing power to ensure the government can protect and defend cyberspace. FAR is a "set of regulations issued by the federal government that specify how Executive Branch agencies are to buy goods and services from commercial vendors."⁷⁰ FAR provides rules that both agencies and vendors must follow when engaging in transactions for the government.⁷¹

For cyber security reasons, if a company wanted to compete for a government contract, the company would have to first comply with the standard FAR rules. It would then have to comply with additional security measures as set out in the FAR to ensure that both the government's networks and the company's systems required for the government contract were secure from cyber attacks.

Any company that cannot meet the government's security standards is eliminated from consideration, thus encouraging compliance if the company wants to do business with the government. Although the procurement process often involves extensive and ongoing communication between the company and the government, this arrangement is not what the team would consider collaboration where parties work together towards a common goal. Rather, the

⁷⁰ "Federal Acquisitions Regulations." Business.Gov: The Official Business Link to the U.S. Government. 19 Aug. 2009 <<http://www.business.gov/expand/government-contracting/far.html>>.

⁷¹ "Federal Acquisitions Regulations."

procurement process is more comparable to negotiations where a party X seeks something from party Y and engages Y in a transaction to meet X's needs in a way that is favorable to X.

Application

While the total dollar amount of government contracts has more than doubled since 2001, reaching over \$500 billion in 2008, the portion of the figure pertaining to cyber is significantly smaller.⁷² Given the enormous size of the worldwide cyber market, not all companies see government business as crucial to the bottom line and consequently do not compete for governmental contracts. Some leading industry corporations conduct only limited business with the government. Representatives from these companies hypothesized that increasing security requirements unique to the government might lead them to cease competing for government contracts.⁷³

Government IT purchases are often stretched over years and may not occur in substantial quantities. Prospective contractors see this as increasing transactional costs that eat away at profits. For example, a company could spend money on one software package developed exclusively for the U.S. government that is delivered over a two year time period. Conversely, the company could also use that same effort to develop a product for worldwide distribution marketed in only a few months. Given how rapid the new product cycle in IT can be, short term efforts and resulting profits will look more attractive to the company than a longer commitment to the government.

⁷² "Memorandum for the Heads of Executive Departments and Agencies". 4 Mar. 2009. 10 Jul. 2009 <http://www.whitehouse.gov/the_press_office/Memorandum-for-the-Heads-of-Executive-Departments-and-Agencies-Subject-Government/>.

⁷³ Hodgkins, Trey. Personal Interview. 9 Jul. 2009.

With more than 4,000 government procurement process statutes already in place, outreach indicated that many companies are hesitant to share information with the government if it results in additional unique government requirements.⁷⁴ Additional rules focused on internet security could discourage potential contract bidders. Furthermore, the 2002 Federal Information Security Management Act (FISMA) already requires federal agencies to strengthen their information and cyber security systems; this includes support and services provided by contractors and others outside the agencies.⁷⁵ Under FISMA, an agency plan must include “policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life-cycle of each organizational information system.”⁷⁶ When an agency engages a contractor for a product or service in the area of information security, the company must meet FISMA security parameters in addition to the usual FAR requirements.

Contractors also expressed concerns about the conflict between FISMA requirements and requirements imposed by international governments and standard-setting bodies. If a higher percentage of a company’s business is outside the U.S. government, there is a business question as to whether meeting U.S. government requirements are cost effective.

Because the procurement system is not precisely intended as a collaborative process, the team did not pursue FAR or FISMA changes as a method for increasing collaboration. However, based on outreach interviews, the team believes that more effort by the U.S. government to establish and implement IT security requirements consistent with international standards could

⁷⁴ Nagle, James F. How to Review a Federal Contract: Understanding and Researching Government Solicitations and Contracts. 2nd ed. Chicago: American Bar Association, 2000. 1.

⁷⁵ “Computer Security Division Computer Security Resource Center: FISMA Detailed Overview.” National Institute of Standards and Technology. 31 Jul. 2009. 14 Aug. 2009 <<http://csrc.nist.gov/groups/SMA/fisma/overview.html>>.

⁷⁶ “Computer Security Division Computer Security Resource Center: FISMA Detailed Overview.”

help ensure that a broad range of the U.S. IT industry continue to compete for government contracts.

DoD AUTHORITIES

A number of government experts raised concerns about limitations on DoD entities to act within a domestic context. The limitations mentioned most often were Title 10, the Posse Comitatus Act, and Title 50.

Title 10

Overview

Article II of the U.S. Constitution provides very broad authority for the President as the Commander in Chief of the Armed Forces to use military power to protect the nation.⁷⁷ The President exercises this authority through civilian and military leaders of the DoD and through issuance of executive branch guidance.⁷⁸ Congress, through Title 10 of the United States Code, defines aspects of how the military is organized and does business. This title provides the legal basis for the roles, missions, and organizations of the Army, Navy, Marine Corps, Air Force, and the Reserve components of all the services.⁷⁹ The U.S. military effectuates Presidential guidance and Title 10 statutory requirements through the issuance of internal rules and directives, strategy documents, and plans and publications that establish within the DoD where authority rests and who can engage in particular operations or activities.⁸⁰

⁷⁷ U.S. Const. Article 11, Cl 11-16. (?)

⁷⁸ The President issues “Executive Orders” (EOs), “Presidential Directives” on various subjects (PDs), “Presidential Decision Directives” (PDDs) and National Strategies to provide executive branch agencies, like DOD, with guidance on how to execute relevant laws and accomplish activities that are directed to them. See, e.g. Presidential Directive (PDD)/NSC-63, Critical Infrastructure Protection, May 22, 1998.

⁷⁹ In addition to providing the legal basis for each of the services, Title 10 also provides the legal basis for General Military Law. 10 U.S.C. Subtitles A-E.

⁸⁰ See, e.g., DOD Directive (DODD) 5525.5, DOD Cooperation with Civilian Law Enforcement Officials (15 Jan. 1986). The rules are further refined by Standing Rules of Engagement, or SROE, and, for a particular operations, by very specific planning and execution orders

From its inception, the U.S. military's prime mission was seen as defending the country from external threats. During outreach, a number of government experts expressed concern that collaboration between the DoD and private sector could lead to activities that exceed Title 10 authorities in that it would involve the DoD in domestic security matters. While it is true that law and tradition have limited the domestic role of the DoD, there is also an extensive history of DoD support to civilian authorities, especially in times of crisis or disaster. The post 9/11 concerns about domestic terrorist threats have also presented additional opportunities for the DoD to support civilian authorities in homeland security operations.⁸¹

Application

Congress has enacted laws enabling entities to request support from the military during domestic operations.⁸² Generally, the kind of support the DoD is authorized to provide includes the provision and operation of DoD equipment and managing the consequences of national disasters. Because the DoD is recognized as the federal agency that is best prepared to defend the Nation's networks, it has been granted increased authority for military involvement in domestic cyber defense.⁸³

For example, the Homeland Security Presidential Directive-7 (HSPD-7) recognized the importance of protecting critical infrastructure. The DoD is specifically designated the lead agency responsible for maintaining and protecting the Defense Industrial Base (DIB).⁸⁴ In response, the DoD issued DoD Directive 3020.40, Defense Critical Infrastructure Program,

⁸¹ Homeland Security is a national effort to prevent further terrorist attacks in the United States, reduce America's vulnerability to terrorism, and if attacks do occur, minimize the damage and enhance recovery. National Strategy for Homeland Security, Office of Homeland Security, Jul. 2002.

⁸² 10 U.S.C. § 371.

⁸³ See Center for Strategic and International Studies, "Securing Cyberspace for the 44th Presidency", Dec. 2008, 23.

⁸⁴ Homeland security Presidential Directive -7, Dec.17, 2003 (7)(a-f),2-3.

which applies to infrastructure identified as necessary to national security.⁸⁵ Under DoD Directive 3020.40, military and non-DoD network assets, including those owned and operated by the private sector, are to be assessed and wherever vulnerabilities are identified, the DoD is authorized to assist DIB companies in addressing those vulnerabilities. While this activity was designed to be proactive rather than forensic in nature, successful protection of the cyber aspects requires information-sharing between the DoD and private sector regarding current cyber incidents on privately owned networks.⁸⁶

The Homeland Security Act of 2002 and the policy implementing HSPD-5 authorized a National Response Plan (NRP).^{87,88} The NRP established a national, comprehensive approach that described the roles of various agencies in planning for and responding to domestic incidents that are national in scale and effect. The NRP, as revised, contains a number of annexes addressing specific types of attacks. The Cyber Incident Annex describes the responsibilities of three federal agencies, the Department of Homeland Security (DHS), Department of Justice (DoJ), and the DoD.⁸⁹ Each agency has core roles and responsibilities related to securing cyberspace and coordinating cyber incident responses. DoD responsibilities flow from the department's competencies in computer security and computer network defense. Among DoD duties under the annex are to "provide attack sensing and warning capabilities, gain attribution of the cyber threat,

⁸⁵ See also, President, "Critical Infrastructure Protection, Presidential Decision Directive-63 May 22, 1998

⁸⁶ There is no question that DOD has authority under Title 10 to protect its own networks and cyber related infrastructure. Collaboration with the private sector for that purpose raises no authority questions. But information-sharing implies an exchange of information useful to both parties. Therefore DOD must be ready to share information with the private sector even where a perceived threat might not have a direct impact on DOD missions. It is this aspect of information-sharing that calls into question the military's authority to participate in purely private sector issues.

⁸⁷ Public Law 107-296, 6 U.S.C. 101 note.

⁸⁸ Effective 15, Dec.2004. The NRP was updated and redesignated as the National Response Framework on Mar. 22, 2008.

⁸⁹ Cyber Incident Annex, National Response Plan(NRP) December 2004 CYB (cyber)-1.

participate in information-sharing, offer mitigation techniques, and perform network intrusion diagnosis and provide technical expertise.”⁹⁰

The role of nongovernmental entities is also recognized in the Cyber Incident Annex. The document acknowledges the importance of involving private sector owners and operators of cyber networks, pointing to the multiple opportunities for government and the private sector to exchange vital security information. Information-sharing across critical sectors is described as necessary to address vulnerabilities and “achieve a higher level of critical infrastructure protection.”⁹¹

Posse Comitatus Act

Overview

But even when government experts were generally familiar with these expanded authorities encouraging the DoD to share information on cyber threats and incidents, they still expressed concern that the type of information-sharing that would be necessary for effective cyber defense would run afoul of the statutory limitations in the Posse Comitatus Act (PCA). Generally, this statute makes it a crime for the military to perform civilian law enforcement functions. Violators are subject to fines, imprisonment, or both.⁹² However, the PCA does not prohibit all military involvement with civilian law enforcement as it contains numerous statutory exceptions.

⁹⁰ Cyber Incident Annex, National Response Plan(NRP) December 2004, Cyber - 6.

⁹¹ Cyber Incident Annex, National Response Plan(NRP) December 2004 Cyber -1.

⁹² 18 U.S. &1385. The PCA was first enacted in 1878 in response to the military presence in the South during post-civil war reconstruction. The term “posse comitatus” is Latin for the “power of the country.” Under English common law it referred to all those over age 15 who could be called on by a sheriff to quell civil disorder. *United States v. Hartley*, 796 F.2d 112, 114, n.3 (5th Cir. 1986). The present version of statute applies only to active duty military members of the Army and Air Force, perhaps in recognition of the role of the Navy plays in enforcing piracy and drug laws. However, 10 U.S.C. & 375 directs the Secretary of Defense to promulgate regulations to prohibit “direct participation by a member of the Army, Navy, Air Force or Marines in a search, seizure, arrest...unless participation is otherwise authorized by law.” See, also, DODD 5525.5.

The three PCA exceptions for military involvement include the following: (1) use of information collected during military operations, (2) loan or lease of military equipment and facilities, and (3) participation of DoD personnel in civilian law enforcement activities.⁹³ Only the first is of concern when dealing with government and private sector information-sharing. In 10 U.S.C. § 371, the Secretary of Defense is allowed to provide information collected during the normal course of military operations to civilian law enforcement agencies if the information is relevant to a violation of state or federal law. In addition, 10 U.S.C. § 371 directs the Secretary of Defense to promptly provide this information to law enforcement authorities as soon as possible. However, the creation or execution of a military mission for the primary purpose of aiding civilian law enforcement officials is prohibited.⁹⁴

Application

The desirable information-sharing is to occur between DoD and cyber networks owners and operators to protect and defend shared systems and to insure that DoD missions and private sector commercial interests are not negatively impacted. This core mission of the DoD is neither created nor executed primarily to assist civilian law enforcement officials. One result of information-sharing may be the identification of individuals or groups who could be guilty of violation for any number of domestic statutes.⁹⁵ Furthermore, 10 U.S.C. § 371 not only allows but encourages the sharing of information with civilian law enforcement officials.

⁹³ 10 U.S.C. § 371-375.

⁹⁴ This is also known as the Military Purpose Doctrine which involves actions taken primarily for military purposes such as protecting DOD personnel and equipment. It is a recognized exception to the PCA. DODD 5525, Sec. E41., 14-15.

⁹⁵ Often in cyber attacks the identity and the purpose of the attack is not readily apparent. An attack can be an act of vandalism, one perpetrated by organized crime, the work of domestic or foreign terrorists, economic espionage or an attack carried out by the military of a hostile nation. Michael A. Vatis, Director, National Infrastructure Protection Center, Federal Bureau of Investigation, Senate Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, Mar. 16, 1999.

In addition, and as discussed above, the Homeland Security Act of 2002 established procedures for the sharing of information necessary to protect the country from acts of military and economic terrorism; those procedures apply to all agencies of the federal government.⁹⁶ Thus, the Homeland Security Act is another statutory exception to the PCA, allowing the DoD and private sector to share information without fear that military personnel could become subject to criminal penalties.

Title 50

Overview

Some government interviewees also cited Title 50 as presenting a legal barrier to collaboration with the private sector. Title 50 of the National Security Act of 1947 establishes a program for national security and defines the role and missions of the various intelligence agencies.⁹⁷

Chapter 36 of Title 50, Foreign Intelligence Surveillance, established the authority for DoD intelligence organizations to conduct intelligence activities. Executive Order (EO) 12333, United States Intelligence Activities, and DoDD 5240.1, DoD Intelligence Activities, implement and further refine the statutory guidance of Title 50 as it pertains to the DoD. These documents make it clear the intelligence mission of military organizations is limited to collecting foreign intelligence and counterintelligence.⁹⁸ Military organizations are generally barred from collecting, retaining or disseminating information about the domestic activities of U.S. persons.

For this reason, even when other DoD components are authorized to provide support to domestic

⁹⁶ HSA of 2002 § 891,892.

⁹⁷ 50 U.S.C. & 401 et seq.

⁹⁸ “Foreign intelligence” is defined as information relating to the capabilities, intentions and activities of foreign powers, organizations or persons. The concept of foreign intelligence does not include counterintelligence, except for information on international terrorist activities. “Counterintelligence” is defined as information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassination conducted for or on behalf of foreign powers, organizations, or persons, or international terrorists activities, but not including personnel, physical, document, or communications security programs. EO 12333, para. 3.4(a),(d) Dec. 4, 1981.

entities, DoD intelligence elements rarely participate. In those instances when military intelligence organizations are authorized to collect foreign intelligence and counterintelligence within the U.S., these activities must still be directed at activities involving a foreign power, organizations, or persons and must be done in coordination with the FBI.⁹⁹

In addition to the statutory limits on intelligence activities, the DoD has issued internal rules that forbid non-intelligence DoD agencies from collecting, processing, and storing information on U.S. individuals and entities not affiliated with the DoD.¹⁰⁰ There are exceptions to the DoD prohibition on intelligence gathering on U.S. persons. The most pertinent exception states that information on U.S. persons can be acquired to protect DoD functions and property.¹⁰¹ For example, if there were a circumstance in which a privately owned cyber network was attacked by a U.S. person or entity, Title 50 would prevent DoD from collecting information. However, if the attack affected DoD functions or property, such as destroying information on DoD computers or interrupting DoD functions, DoD personnel other than intelligence units could collect, process, and store information on the perpetrator.¹⁰² This limited authorization for DoD non-intelligence units to collect information on U.S. persons when DoD property and programs are at risk appears sufficient to alleviate the stated Title 50 concerns of the government experts.

⁹⁹ Executive Order 12333, para 1.14(a). See also discussion of the Patriot Act, the Federal Wiretap Act and the Federal Intelligence Surveillance Act above.

¹⁰⁰ DODD 5200.27 “Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense.

¹⁰¹ DODD 5240.1, DOD Intelligence Activities (Apr. 25, 1998)

¹⁰² DODD 5200.27 is clear that even where authorized the collection should be conducted in a manner that is least intrusive and that seeks to honor constitutional and privacy rights. In addition, Information collected must be destroyed within 90 days unless further retention is required by law or authorized.

Application

Outreach interviews left the research team with the clear impression that many experts, especially DoD experts, were unclear or confused about DoD authority to participate in cyber defense collaboration with the private sector. The issues of DoD authorities in the cyber arena are complex. The team recommends the DoD General Counsel be asked to issue an advisory opinion, available to all parties, explaining the parameters of DoD authorities in this area of law.

LAWS AFFECTING BUSINESS PROPERTY AND COMPETITION

During outreach, intellectual property concerns and antitrust laws were cited as potential barriers to collaboration. These two areas of law affect the way businesses interact and compete with one another. Intellectual property encompasses three bodies of law: patents, trademarks, and copyrights. Antitrust law seeks to prevent businesses from interacting in such a way to negatively affect the market.

Intellectual Property

Intellectual Property consists of patents, trade secrets, trademarks, and copyrights.¹⁰³ Not all areas of intellectual property present barriers to collaboration, but whether or not, and in what way, a type of intellectual property affects collaboration is discussed below.

Patents & Trade Secrets

Overview

Article 1, § 8, clause 8 of the United States Constitution states “[t]he Congress shall have power...to promote the progress of...useful arts, by securing for limited times to...inventors the exclusive right, to their...discoveries.”¹⁰⁴ A patent grants to the inventor of a product a property right in the invention.¹⁰⁵

Generally, the Patent Act mandates that an individual attempting to obtain a patent must demonstrate on a patent application that he has created a novel, non-obvious, and useful product

¹⁰³ Miller, Arthur R., and Davis, Michael H. Intellectual Property: Patents, Trademarks, and Copyright, In a Nut Shell. 4th ed. St. Paul, MN: West Publishing Company, 1990.

¹⁰⁴ 35 U.S.C. 1-376

¹⁰⁵ “General Information Concerning Patents.” United States Patent and Trademark Office. Jan. 2005. 14 Aug. 2009 <<http://www.uspto.gov/go/pac/doc/general/#patent>>.

or process. First, the patentee must describe how the product operates. Second, the patentee asserts “claims,” which are actual patentable attributes of the product. The claims must demonstrate the product is an invention in part by indicating whether the claims are novel, non-obvious, or useful advancements. The term “useful” means the invention must have a useful purpose.¹⁰⁶ Mere ideas are not patentable.¹⁰⁷ The Patent Office makes the determination of whether or not a product or process is patentable.

The patent system was created in part to encourage the development of technology. Patent applications are public documents that are stored by the Patent Office, and provide notice to the public about new inventions. Once a patent is properly granted, the patentee has the exclusive right to determine who, if anyone, has the right to use, make, sell, or offer to sell the invention during the length of the patent.¹⁰⁸ The patent is valid for 20 years from the date of original application. Some inventions, such as drugs and medical devices, are extendable for up five years if certain conditions are met. When the 20-year patent expires, an invention becomes available for public use because a patent cannot be renewed. The former patent holder no longer has the exclusive right to sell, use, offer, or make the invention.¹⁰⁹

Patents are often confused or grouped with the intellectual property law known as trade secrets.

The Uniform Trade Secret Act (USTA) defines trade secrets as:

¹⁰⁶ General Information Concerning Patents.” United States Patent and Trademark Office. Jan. 2005. 14 Aug. 2009 <<http://www.uspto.gov/go/pac/doc/general/#patent>>.

¹⁰⁷ General Information Concerning Patents.”

¹⁰⁸ Miller, Arthur R., and Davis, Michael H. Intellectual Property: Patents, Trademarks, and Copyright, In a Nut Shell. 4th ed. St. Paul, MN: West Publishing Company, 1990. In order for an invention to receive a patent, it must be an invention type listed in § 101 of the Patent Act. Section 101 states “[w]hoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefore, subject to the conditions and requirements of this title.” First, a utility patent is granted to an inventor of a new and useful machine, process, or article of manufacture. Second, a design patent is granted to a new and original design. Third, a plant patent is granted to an inventor of an asexually reproducing or new type of plant. “General Information Concerning Patents.” United States Patent and Trademark Office. Jan. 2005. 14 Aug. 2009 <<http://www.uspto.gov/go/pac/doc/general/#patent>>.

¹⁰⁹ “General Information Concerning Patents.” United States Patent and Trademark Office. Jan. 2005. 14 Aug. 2009 <<http://www.uspto.gov/go/pac/doc/general/#patent>>.

information, including a formula, pattern, compilation, program device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.¹¹⁰

For information to be considered a trade secret, it must remain a secret. For example, the Coca-Cola recipe is a trade secret because the recipe has been kept a secret for over 100 years to protect Coca-Cola's economic interests.¹¹¹

Application

During outreach, intellectual property, most particularly concerns about trade secrets, was mentioned as a factor the private sector considers as inhibiting collaboration. The emphasis on trade secrets as opposed to patents is understandable. A trade secret protects information by keeping it a secret and a patent protects information by disclosing it.¹¹² A major patent requirement is that information be available to the public. Therefore, all information related to a patent is made publically available when the patent is granted. Patented information does not significantly affect collaboration between that organization and the government; however, the collaboration itself should not involve any patent infringement actions.

If a private sector organization has a trade secret, such as software codes or security processes, this could create a barrier to collaboration with the government as it will be based, in large part, on information-sharing that could involve trade secret information. Thus, if the government

¹¹⁰ Uniform Trade Secrets Act of 1979 § 1(4), 14 U.L.A. 542 (1979).

¹¹¹ "Trade Secrets v. Patents." Invention Resource International. 14 Aug. 2009

<http://www.inventionresource.com/index.php?option=com_content&view=article&id=37>.

¹¹² Hosteny, Joseph N. "Litigators Corner: Patent or Trade Secret: Which one is Best?" Joseph Hosteny: Intellectual Property Attorney. 14 Aug. 2009 <<http://www.hosteny.com/archive/hosteny%2008-00.pdf>>.

wishes to collaborate, it will be necessary for government collaborators to understand and evidence the ability to protect trade secret properties of private sector parties. In addition, trade secret concerns may inhibit broad based collaboration among horizontal competitors in the cyber industry, meaning the desire to protect trade secrets could prevent information-sharing among similar corporations.

Trademarks

Overview

Trademark protection dates back to the medieval period when guild members stamped their guild mark on goods they were selling. The mark provided notice of the craftsman or group of craftsmen who created the good.¹¹³ The trademark was also a means to gain a competitive edge over other craftsmen.

Generally, a trademark is a name or logo that is attached to a product that a consumer would associate with that product, or a recognizable packaging of a product.¹¹⁴ A trademark of a good does not exist on its own, but rather it always exists in connection with commercial activity. This means that absent the sale of goods, a trademark has no meaning or effect.

Unlike patents and copyrights, trademarks were designed to prevent deception with regard to a good's origin. In this way trademarks protect the competitive advantage of the seller and protect the consumer by preventing confusion as to whose product they are buying.

¹¹³ Miller, Arthur R., and Davis, Michael H. Intellectual Property: Patents, Trademarks, and Copyright, In a Nut Shell. 4th ed. St. Paul, MN: West Publishing Company, 1990.

¹¹⁴ 41 CRLR 515; H.R. Rep. No. 109-23, at 4 (2005), as reprinted in 2006 U.S.C.C.A.N. 1091, 1092.

A trademark is infringed if there is a “likelihood of confusion.”¹¹⁵ Essentially, the claim requires that the infringer use a word or symbol that is identical or confusingly similar to another’s goods in commerce without a right to do so and is likely to cause, or causes, confusion as to its origin. The burden of proof to demonstrate an infringement is low because the requirement is a likelihood of confusion, rather than actual confusion.¹¹⁶ There are several factors that are considered to determine likelihood of confusion, including but not limited to, similarity of services and goods, actual confusion, and similarity of markings.¹¹⁷

Application

Trademarks could be involved in the cyber domain. For instance, if a hacker or phisher utilizes a company’s logo or mark to entice computer users to a bogus site, that use would constitute a trademark infringement. But trademark concerns are not implicated in a voluntary sharing of cyber security data, nor would it be likely that the collaboration would utilize private sector trademarks. In fact, the collaboration could result in more efficient ways to identify and prevent infringement of trademarks.

Copyrights

Overview

Like patents, copyrights are a method to protect the commercial value of something that is within the public domain.¹¹⁸ Copyrights provide protection for original works in order to assure the author receives benefit for his or her creativity.¹¹⁹ Copyright protection is not applicable to

¹¹⁵ Miller, Arthur R., and Davis, Michael H. Intellectual Property: Patents, Trademarks, and Copyright, In a Nut Shell. 4th ed. St. Paul, MN: West Publishing Company, 1990.

¹¹⁶ Miller, Arthur R., and Davis, Michael H.

¹¹⁷ Miller, Arthur R., and Davis, Michael H.

¹¹⁸ “A Brief Introduction and History.” Library of Congress: United States Copyright Office. 14 Aug. 2009 <http://www.copyright.gov/circs/circ1a.html>>.

¹¹⁹ Yen, Alfred C. and Joseph P. Liu. Copyright Law: Essential Cases and Materials. St.Paul, MN: Thomas/West, 2008.

ideas.¹²⁰ A work must be in a fixed form in order to receive copyright protection, that is when it is “sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated.”¹²¹ For example, a drawing on a napkin is sufficiently permanent to receive copyright protection.¹²²

There are many types of works that cannot receive copyright protection. Facts and mere copying are not subject to copyright protection. In this way, phone numbers are not copyrightable, but if the arrangement of the numbers in a book or online listing meets the minimum threshold for creativity, then the arrangement of phone numbers might be copyrightable. Copyright protection is not applicable to ideas. A copyright does not extend to “any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which its described, explained, illustrated, or embodied.”¹²³ To be protected under copyright, a work must be artistic and utilitarian.

The holder of a copyright has many exclusive rights, such as the right to reproduce and sell copies of the work.¹²⁴ A copyright is infringed when anyone violates any of these exclusive rights. For example, when computer software is sold to the public it is usually copyrighted to prevent it from being copied or resold.

Application

The issue of copyright infringement was not discussed during outreach efforts, perhaps because copyrighted materials are already in the public domain and collaboration among competitors or with the government should not increase the likelihood of copyright infringement. Moreover,

¹²⁰ Miller, Arthur R., and Davis, Michael H. Intellectual Property: Patents, Trademarks, and Copyright, In a Nut Shell. 4th ed. St. Paul, MN: West Publishing Company, 1990.

¹²¹ 17 U.S.C. 101

¹²² Yen, Alfred C. and Joseph P. Liu. Copyright Law: Essential Cases and Materials. St. Paul, MN: Thomas/West, 2008.

¹²³ 17 U.S.C. 102(b).

¹²⁴ 17 U.S.C. 106

increasing cyber security may develop improvements to copyrighted security that could prevent pirating of copyrighted software.

Antitrust: The Sherman Act

Overview

During outreach, several companies expressed reservations at the idea of meeting with their competitors to discuss threats affecting their networks and infrastructure security or other cyber vulnerabilities. Such reservations stemmed from fear of violating antitrust laws that can result in criminal and civil penalties.

Section 1 of the Sherman Act states:

Every contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce among the several States, or with foreign nations, is declared to be illegal. Every person who shall make any contract or engage in any combination or conspiracy hereby declared to be illegal shall be deemed guilty of a felony.¹²⁵

The concept “conspiracy in the offense” means a company can violate the Sherman Act even if there was no intent to restrict trade or if the attempt was not successful. Business representatives indicated in outreach that companies are concerned about sitting down at the table with their competition for anything more than a casual conversation for fear such a meeting would be seen as a conspiracy to violate antitrust laws.

Antitrust law centers on the idea that society is better off when markets are competitive.¹²⁶

Society is presumably harmed, if a few companies control the market and there is no

¹²⁵ 15 U.S.C § 1

¹²⁶ 15 U.S.C § 1

competition. Antitrust laws have multiple channels for lawsuits to be lodged against offending companies, and violators face monetary fines and possible jail time. As stated by one antitrust expert, “Congress has put teeth into section 1 that can prove both sharp and painful for those caught violating the Act.”¹²⁷ Accordingly, companies are extremely cautious as they want to avoid even the appearance of violating antitrust laws.

Any person that is injured by a violation of antitrust laws may bring a civil suit in federal district court to recover treble damages plus costs and attorney’s fees.¹²⁸ Foreign nationals can also bring suit.¹²⁹ State Attorney Generals may file a civil suit against a company on behalf of state citizens and also collect treble damages.¹³⁰ Finally, the DoJ may bring a criminal case against those violating § 1 of the Sherman Act. A guilty verdict could lead to a maximum fine of \$100 million for corporations and \$1 million for individuals.¹³¹ Violation of the Sherman Act is a felony; officials of a competitive company who participate in antitrust activities can be punished by jail sentences for up to 10 years.¹³² Antitrust violations, therefore, can lead to substantial penalties as at least three potential parties can sue based on a single violation: private individuals, state Attorney Generals, and the DoJ.

Key to any Sherman Act § 1 analysis is the requirement of a “concerted action” by two or more parties. The court must analyze whether the conduct “consists of concerted action or the merely unilateral behavior of separate actors.”¹³³ Thousands of U.S. companies take action to protect their cyber networks. At any one time hundreds may be engaged in the identical act in response

¹²⁷ Holmes, William C. Antitrust Law Handbook. 2008-09 ed. Thomson West, 2008. pg 100.

¹²⁸ 15 U.S.C. § 15(a)

¹²⁹ 15 U.S.C § 15(b)(1)

¹³⁰ 15 U.S.C § 15(c)

¹³¹ 15 U.S.C. § 1.

¹³² The U.S. Government through the Justice Department can bring criminal enforcement cases under the Sherman Act. 15 U.S.C. § 1,2.

¹³³ Holmes, William C. Antitrust Law Handbook. 2008-09 ed. Thomson West, 2008. pg 101

to a broad-based cyber attack. Individual acts do not give rise to antitrust violations, but many businesses fear that conversing with competitors about the actions being taken might give the appearance of concerted action. For an actual antitrust violation, however, the complaining party must prove the concerted action “had a conscious commitment to a common scheme designed to achieve an unlawful objective.”¹³⁴ In other words, the alleged offender must take willful steps toward an illegal act or an act that reduces competition in the market.

As the U.S. Supreme Court noted in one of the earliest antitrust cases, *Chicago Board of Trade v. United States*, “every agreement concerning trade, every regulation, restrains” but not all agreements are violations.¹³⁵ In 1997, the U.S. Supreme Court detailed the modern application of the ‘restraint on trade’ language in the case *State Oil Company v. Khan*, quoted below.¹³⁶

Although the Sherman Act, by its terms, prohibits every agreement “in restraint of trade,” this Court has long recognized that Congress intended to outlaw only unreasonable restraints. As a consequence, most antitrust claims are analyzed under a “rule of reason,” according to which the finder of fact must decide whether the questioned practice imposes an unreasonable restraint on competition, taking into account a variety of factors, including specific information about the relevant business, its condition before and after the restraint was imposed, and the restraint's history, nature, and effect (cites omitted).¹³⁷

¹³⁴ *Edward J. Sweeney & Sons*, at 111; accord *H.L. Moore Drug Exchange v. Eli Lilly & Co.*, 662 F.2d 935, 941 (CA2 1981) cert. denied, 459 U.S. 880, 103 S.Ct. 176, 74 L.Ed.2d 144 (1982); cf. *American Tobacco Co. v. United States*, 328 U.S. 781, 810, 66 S.Ct. 1125, 1139, 90 L.Ed. 1575 (1946) in *Monsanto Co. v. Spray-Rite Service Corp.*, 465 U.S. 752, 104 S.Ct. 1464 at 764 (1984).

¹³⁵ 246 U.S. 231, 238 (1918)

¹³⁶ 522 U.S. 3, 10 (1997).

¹³⁷ See, e.g., *Arizona v. Maricopa County Medical Soc.*, 457 U.S. 332, 342-343, 102 S.Ct. 2466, 2472-2473, 73 L.Ed.2d 48 (1982) (citing *United States v. Joint Traffic Assn.*, 171 U.S. 505, 19 S.Ct. 25, 43 L.Ed. 259 (1898)). 457 U.S., at 343, and n. 13, 102 S.Ct., at 2472, and n. 13 (citing *Board of Trade of Chicago v. United States*, 246 U.S. 231, 238, 38 S.Ct. 242, 243-244, 62 L.Ed. 683 (1918)).

This analysis, known as the rule of reason, allows competitors to meet and even agree to act as long as their agreement and the actions that they take help achieve a legitimate business purpose that is not price-fixing, a boycott, or other anticompetitive consequences.¹³⁸

Some agreements by businesses, however, cannot rely on the rule of reason test as some business activities constitute a “per se” violation of the Sherman Act. A per se violation indicates that the very nature of the restraint on trade is in itself a violation. The restraint has no positive effect on competition and courts have dealt with the anticompetitive harm of the restraint so often that such acts are essentially treated as violating § 1 of the Sherman Act, as the Supreme Court discussed in *State Oil*:

Some types of restraints, however, have such predictable and pernicious anticompetitive effect, and such limited potential for procompetitive benefit, that they are deemed unlawful *per se*. *Per se* treatment is appropriate ‘[o]nce experience with a particular kind of restraint enables the Court to predict with confidence that the rule of reason will condemn it.’ Thus, we have expressed reluctance to adopt per se rules with regard to ‘restraints imposed in the context of business relationships where the economic impact of certain practices is not immediately obvious.’ (citations omitted).¹³⁹

Some of the most common per se violations include agreements for price fixing, horizontal agreements, territorial allocations, and boycotts.¹⁴⁰ Such agreements almost always raise prices

¹³⁸ Gellhorn, Ernest, William E. Kovacic, Stephen Calkins. Antitrust Law and Economics, 5th ed. Minnesota: West Publishing Co., 1994.

¹³⁹ *State Oil* at 10 citing *Northern Pacific R. Co. v. United States*, 356 U.S. 1, 5, 78 S.Ct. 514, 518, 2 L.Ed.2d 545 (1958). See also *Broadcast Music, Inc. v. Columbia Broadcasting System, Inc.*, 441 U.S. 1, 19, n. 33, 99 S.Ct. 1551, 1562 n. 33, 60 L.Ed.2d 1 (1979). *FTC v. Indiana Federation of Dentists*, 476 U.S. 447, 458-459, 106 S.Ct. 2009, 2018, 90 L.Ed.2d 445 (1986).

¹⁴⁰ Federal Trade Commission and U.S. Department of Justice. Antitrust Guidelines for Competition Among Competitors. 2000. 30 Jul. 2009. <<http://www.ftc.gov/os/2000/04/ftcdojguidelines.pdf>>

or reduce output.¹⁴¹ But if the economic impact of the restraint of trade is not obvious, the restraint is no longer a per se violation but will be analyzed under the rule of reason.

Application

Although members of the private sector were somewhat ambivalent about meeting with their competitors to engage in information-sharing on network threats and vulnerabilities, they were explicit in the concern about violating antitrust law if such a meeting took place. It is clear that information-sharing on cyber security should not result in higher prices, a reduction in output, or a territorial allocation, but if companies meet with their competitors, they may be concerned with an allegation of a boycott or horizontal agreement.

For example, companies A and B could share information regarding network threats and vulnerabilities. This could lead to better security and efficiency for these two companies. However, if company C is not allowed to take part in the information-sharing, this could be construed as an anticompetitive act by A and B. Company C might then try to show that A and B were involved in a boycott to deprive C of effective competition with A and B.

As this example illustrates, the private sector companies' fears are not unreasonable. In order to share information, companies would need to meet or at least communicate with each other, which could feasibly raise a boycott issue as it would not be practical to invite all competitors to the same session. However, boycott issues would not be implicated if the companies were meeting solely for information-sharing. The meetings focusing on network threats and vulnerabilities, and not agreements to refuse business to another company would likely be permissible under the Sherman Act.

¹⁴¹ Federal Trade Commission and U.S. Department of Justice. Antitrust Guidelines for Competition Among Competitors. 2000. 30 Jul. 2009. <<http://www.ftc.gov/os/2000/04/ftcdojguidelines.pdf>.>

If as a result of an information-sharing meeting, companies A and B agree to the standardization of their individual activities or agreed to share new products or services, this could raise questions about anticompetitive actions by A and B.¹⁴² New requirements for their products or standardization between the two could adversely affect the market, and A and B might be accused of violating antitrust laws. However, as long as the meeting was carefully crafted to be limited solely to information-sharing on threats to the companies' networks and infrastructure, antitrust challenges would likely not occur.

It is not apparent that companies should be worried about being accused of rule of reason violations. Consumers can benefit from competitor collaborations that result in cheaper goods and services or products getting to the market faster.¹⁴³ Information-sharing, if it increases efficiency or improves a product, could allow companies to lower prices. Concerted actions that benefit the consumer often receive kind treatment by the courts. An action is likely to raise antitrust suspicions if there is an agreement to decrease output, establish prices, reduce a company's incentive or ability to compete independently, or allocate market share.¹⁴⁴ Again, the sharing of information alone should not affect market share, prices, or outputs. Information-sharing related to the protection of cyberspace would focus on threats to networks and infrastructure, system vulnerabilities, and data security. Although each of these cyber business aspects could be improved through information the companies gleaned from collaboration, individual actions by a company not in concert with competitors to improve products would encourage competition and benefit the consumer. In analyzing Sherman Act violations, the

¹⁴² Federal Trade Commission and U.S. Department of Justice. Antitrust Guidelines for Competition Among Competitors. 2000. 30 Jul. 2009. <<http://www.ftc.gov/os/2000/04/ftcdojguidelines.pdf>>.

¹⁴³ Federal Trade Commission and U.S. Department of Justice. Antitrust Guidelines for Competition Among Competitors. 2000. 30 Jul. 2009. <<http://www.ftc.gov/os/2000/04/ftcdojguidelines.pdf>>.

¹⁴⁴ Holmes, William C. Antitrust Law Handbook. 2008-09 ed. Thomson West, 2008. pg 6

Supreme Court has looked favorably upon acts that resulted in lower prices and has stated that an attempt to lower cost is the epitome of competition:

‘Low prices,’ we have explained, ‘benefit consumers regardless of how those prices are set, and so long as they are above predatory levels, they do not threaten competition.’ Our interpretation of the Sherman Act also incorporates the notion that condemnation of practices resulting in lower prices to consumers is ‘especially costly’ because ‘cutting prices in order to increase business often is the very essence of competition (citations omitted).’¹⁴⁵

Although it appears that the type of information-sharing that the DoD needs for cyber security purposes does not implicate Antitrust Laws, the frequency and consistency of antitrust concerns expressed by outreach experts indicates how the fear of violating the Sherman Act is ingrained in corporate culture. In order to encourage collaboration with the private sector, the government will need to overcome this understandable mindset. This could be done by carefully structuring the meetings and the type of information to be exchanged. Specific recommendations to address antitrust concerns are discussed in the Recommendations section of this report.

¹⁴⁵ *State Oil*, at 15 citing *Atlantic Richfield Co. v. USA Petroleum Co.*, 495 U.S. 328, 110 S.Ct. 1884 109 L.Ed.2d 333(1990), at 340, 110 S.Ct., at 1892; *Matsushita Elec. Industrial Co. v. Zenith Radio Corp.*, 475 U.S. 574, 594, 106 S.Ct. 1348, 1360, 89 L.Ed.2d 538 (1986).

PUBLIC ACCESS TO GOVERNMENT INFORMATION

A foundational principle of U.S. democracy is government transparency. This requires broad public access to government information. The primary statutes related to federal information policy are the FOIA, and FACA.

FOIA

Overview

FOIA is a law that will be implicated if the government and private sector collaborate to protect and defend cyberspace. The law requires the government to disclose records under its control, and it also allows the withholding of certain records under a number of exemptions that protect certain kinds of information.

When speaking with outreach interviewees from the private sector, FOIA was cited as one of the major influences impacting the trust relationship between the government and the private sector.¹⁴⁶ The private sector is often unwilling to share sensitive business information with the government for fear it will be released to the public. If disclosed, the information could have significant negative consequences, such as jeopardizing the public opinion of the company's stability, or the dissemination of key vulnerabilities. This reluctance is easily understood given the broad nature of FOIA's reach. Anyone may submit a request to a federal agency for any record controlled by the agency, and the agency must provide that record subject to certain exclusions and exemptions.¹⁴⁷ FOIA only requires disclosure of "agency records." The term

¹⁴⁶ Daniel Ryan. Personal Interview. 16 Jun. 2009.

¹⁴⁷ FOIA does not apply to all parts of the executive branch or to all "records." Only an "agency," as defined under the Administrative Procedure Act ("APA") is subject to the FOIA.

“record” is “any information that would be an agency record subject to the requirements of this section when maintained by an agency in any format, including an electronic format.”¹⁴⁸ The U.S. Supreme Court, in *Department of Justice v. Tax Analysts*, defined the term “agency record” using a two-part test, and stated that a record is an “agency record” if it is created or obtained by an agency, and in the agency’s control.¹⁴⁹ Other court opinions have established that the question of “agency control” turns on four factors: (1) the intent of the document’s creator to retain control over the record, (2) the ability of the agency to use and dispose of the record as it sees fit, (3) the extent to which agency personnel have read or relied upon the document, and (4) the degree to which the document was integrated into the agency’s record system or files.¹⁵⁰ Thus, documents regarding the protection and defense of cyberspace, created by the private sector and submitted or shared with the government could become agency records subject to the disclosure requirements of FOIA, unless that record falls within an exemption.¹⁵¹ In total, nine exemptions are provided.¹⁵²

Exemptions

Exemption One provides that FOIA does not apply to matters that are properly classified. Only “if a document has been properly classified under a Presidential Executive order” can the document be withheld from disclosure.¹⁵³ Particularly relevant to this project is Executive Order 13292, which expands the protection to information concerning terrorism. Executive Order 13292 permits the classification of “scientific, technological, or economic matters relating to the

¹⁴⁸ 5 U.S.C. §552(f)(2)

¹⁴⁹ *Department of Justice v. Tax Analysts*, 492 U.S. 136, 144-46 (1989).

¹⁵⁰ *Burka v. Department of Health and Human Services*, 87 F.3d 508, 515 (D.C. Cir. 1996).

¹⁵¹ 5 U.S.C. § 552(b)(1) through (9), as amended by Pub. L. 110-175.

¹⁵² 5 U.S.C. § 552§ 552(b)(1)

¹⁵³ *A Citizen’s Guide on Using the Freedom of Information Act and the Privacy Act of 1974 to Request Government Records*, H. Rep. No 108-372, at 15, 107th Cong., 2d Sess. (2002).

national security, which includes the defense against transnational terrorism.”¹⁵⁴ To encourage cyber collaboration, an amendment to Executive Order 13292 focused on the protection and defense of cyberspace would allow for the inclusion of critical infrastructure information relating to e-threats and vulnerabilities within the definition of “national security.” In this way, documents and electronic records exchanged between the government and private sector would be exempt from disclosure. The inclusion of this information would facilitate the collaboration between the government and private sector when sharing information relating to cyber threats and vulnerabilities. The fear harbored by the private sector that information will be disclosed under FOIA would be mitigated by Exemption One’s protection of this information. However, classification is a doubled-edged sword. Once information is classified, dissemination among collaborating parties is restricted. The Culture section of this report discusses the private sector concerns with over-classification of information by the government. Given these concerns, the team does not believe that an Executive Order specifically allowing the classification of this type of information is the best approach.

Exemption Two of the FOIA allows the withholding of information that relates to an agency’s internal practices and personnel rules.¹⁵⁵ Exemption Two applies to information that is “trivial administrative information in which the public should have little interest and would be burdensome for an agency to produce.”¹⁵⁶ It is unlikely that Exemption Two can be relied on as a means of withholding shared cyber security information.

Exemption Three applies to matters that are “specifically exempted from disclosure by statute, provided that such statute do one of the following two things: (1) requires that the matters be

¹⁵⁴ Executive Order No. 13292, Sec. 1.1(4)

¹⁵⁵ 5 U.S.C. § 552(b)(2)

¹⁵⁶ Gidiere III, P. S. (2006). *The federal information manual*. Chicago: ABA Publishing, p. 227.

withheld from the public in such a manner as to leave no discretion on the issue; or (2) establishes particular criteria for withholding, or refers to particular types of matters to be withheld.”¹⁵⁷ Many federal statutes other than FOIA deal with the government’s authority to withhold information from the public. Exemption Three recognizes this fact and incorporates those statutes by reference. Examples of such statutes include those that protect financial disclosure information submitted to a bank regulatory agency, and that protect unclassified technical data with military or space applications.^{158 159} There currently exists no Exemption Three statute that protects information obtained from a third party that concerns cyber security. If a statute outside of FOIA was enacted that specifically exempted from disclosure information on e-threats and vulnerabilities, Exemption Three would incorporate that statute into FOIA and protect such information from disclosure. Such an exemption would clearly establish the ability of the government to safeguard information shared by collaborating sector partners when protecting and defending cyberspace.

Exemption Four protects privileged or confidential trade secrets and commercial or financial information obtained from a person.¹⁶⁰ Exemption Four applies to information that contains trade secrets. A trade secret is generally understood to be information that is kept confidential to maintain an advantage over competitors. This information can include a formula, pattern, program, device, *method*, technique, or *process* (emphasis added). Further, this secret information must derive independent economic value from not being known or readily

¹⁵⁷ 5 U.S.C. § 552(b)(3)

¹⁵⁸ Title 5 § 107(a)(2)

¹⁵⁹ Title 10 § 130

¹⁶⁰ 5 U.S.C. § 552(b)(4).

ascertainable by others. The “owner” of this information must take reasonable efforts to maintain its secrecy.¹⁶¹

Exemption Four has been interpreted to also protect Confidential Business Information (CBI).

“To qualify as CBI, information must be confidential commercial or financial information obtained from a third party not part of the Federal government.”¹⁶² The term confidential means if information were released it would “cause substantial harm to the competitive position of the person from whom the information was obtained.”¹⁶³ An example of CBI in cyber security cooperation might be customer lists and internet addresses.

Exemption Four may offer the most applicable exemption for collaboration between the government and private sector. Information is properly defined as CBI if it is commercial or financial information, obtained from a person, and not released to the public.¹⁶⁴ Under this definition, information is broadly understood as “commercial” when it is “pertaining or relating to or dealing with commerce,” and “person” includes “a wide range of entities including corporations, associations and public or private organizations other than agencies.”¹⁶⁵ The difficulty of this test comes in deciding whether or not the information is confidential. The test for if information is confidential was developed by the court in *National Parks & Conservation Association v. Morton*.¹⁶⁶ This case established that information is confidential if disclosure of information is likely to impair the government’s ability to obtain such information in the future,

¹⁶¹ “Trade Secret.” *Black’s Law Dictionary*, 8th ed. 2004.

¹⁶² *GC Micro Corp. v. Defense Logistics Agency*, 33 F.3d 1109, 1112 (9th Cir. 1994).

¹⁶³ *National Parks & Conservation Association v. Morton*, 498 F.2d 765, 770 (D.C. Cir. 1974). Exemption Four also protects privileged information, defined as information related to special legal rights or exemptions granted to a person. Examples of this privilege include attorney-client privilege, attorney work-product doctrine, and confidential report privilege. This prong of Exemption Four is not implicated in an information-sharing collaboration between the government and private sector.

¹⁶⁴ *GC Micro Corp. v. Defense Logistics Agency*, 33 F.3d 1109, 1112 (9th Cir. 1994)

¹⁶⁵ *Gilmore v. Department of Energy*, 4 F. Supp. 2d 912, 922 (N.D. Cal. 1998)

¹⁶⁶ *National parks & Cons. Ass’n v. Morton*, 498 F.2d 765 (D.C. Cir. 1974)

or will cause substantial harm to the competitive position of the person from whom the information was obtained.

In addition, to qualify for Exemption Four protection, the information in question must be information that was submitted to the government voluntarily.¹⁶⁷ Voluntarily submitted information is protected from disclosure if it is information that “for whatever reason, would customarily not be released to the public by the person from whom it was obtained.”¹⁶⁸ Since the nature of cyber collaboration relies on voluntary action, Exemption Four protection remains an option to protect information from private sector partners. It does not, however, protect government records made part of the collaboration.

Exemption Five applies to “inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency.”¹⁶⁹ This exemption requires the source of the information “must be a Government agency, and it must fall within the ambit of a privilege against discovery under judicial standards that would govern litigation against the agency that holds it.”¹⁷⁰ The collaboration between the government and private sector would require the submittal of information from both the government and private sector. The goal of collaboration is to create a forum where all parties involved advance the quality of the information available to the collaboration. Accordingly, from the government’s perspective, sharing information in a collaborative forum would not be ideal in that when the information is shared, the protection offered under Exemption Five may be forfeited, as the document is no longer an inter- or intra-agency document. The government would essentially be

¹⁶⁷ Critical Mass Energy Project v. Nuclear Regulatory Commission, 975 F.2d 871 (D.C. Cir. 1992).

¹⁶⁸ Critical Mass, 975 F.2d. at 878 (D.C. Cir. 1992)

¹⁶⁹ Title 5 § 552(b)(5)

¹⁷⁰ Department of the Interior v. Klamath Water Users, 532 U.S. 1, 8 (2001).

waiving its ability to claim Exemption Five protection for the documents shared. This could reduce the government's incentive to collaborate.

Exemption Six is concerned with “personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.”¹⁷¹ This provision ensures that personally identifiable information is exempt from disclosure. In regards to the cyberspace collaboration between the government and private sector, Exemption Six does not appear applicable, as it should be possible to collaborate on cyber threats without exchanging personally identifiable information. For example, if Internet Protocol (IP) addresses were revealed by the private sector and could not be withheld under Exemption Four, there is an argument the IP address might constitute personally identifiable information and Exemption Six might come into play.

Exemption Seven applies to information and records that are compiled for the purpose of law enforcement.¹⁷² The focus of Exemption Seven is on the harm that could result from the release of information, such as interference with law enforcement and an unwarranted invasion of personal privacy.¹⁷³ Exemption Seven is not particularly relevant to a non-law enforcement collaboration between the DoD and private sector.

Exemption Eight relates to information “contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions.”¹⁷⁴ Only agencies that regulate financial institutions can use this exemption.

¹⁷¹ Title 5 § 552(b)(6)

¹⁷² Title 5 § 552(b)(7)

¹⁷³ Gidiere III, P. S. (2006). *The federal information manual*. Chicago: ABA Publishing. p. 263

¹⁷⁴ Title 5 § 552(b)(8)

Finally, Exemption Nine deals with “geological and geophysical information and data, including maps, concerning wells.”¹⁷⁵ Exemption Nine is rarely used, and when it is, is most often used by the Environmental Protection Agency. This exemption is not germane to collaboration between the government and private sector to protect and defend cyberspace.

In addition to the nine exemptions mentioned above, FOIA has three exclusions that remove certain records from coverage of the statute. These three exclusions cover sensitive law enforcement information and could be used by a government agency to safeguard information that is being used in the ongoing investigation of cyberspace criminal behavior.¹⁷⁶ But the sensitive law enforcement information would not reach the DoD and private sector collaboration as the DoD has no law enforcement duties, except in the narrow instance where the information pertains to destruction of DoD property and interference with DoD missions. Even in that case, the DoD would turn such information over to law enforcement agencies and refer the FOIA requester to those entities.

In 2002, Congress passed the Homeland Security Act, which detailed an added exemption of FOIA in order to protect “voluntarily submitted critical infrastructure information.”¹⁷⁷ This exemption states that “critical infrastructure information (including the identity of the submitting person or entity) that is voluntarily submitted to the Department of Homeland Security (DHS) for use by DHS regarding the security of critical infrastructure shall be exempt from disclosure.”¹⁷⁸ Following the passage of, and pursuant to, this section, the DHS created the Protected Critical Infrastructure Protection (CIP) program. This program created procedures for the receipt, care, and storage of Critical Infrastructure Information (CII) voluntarily submitted to DHS.

¹⁷⁵ Title 5 § 552(b)(9)

¹⁷⁶ Title 5 § 552(c)(1) through (3)

¹⁷⁷ Homeland Security Act of 2002, Sections 212-215. The nation’s cyber infrastructure is considered critical.

¹⁷⁸ *Homeland Security Act of 2002* at Sec. 214(a)(1)

Information submitted voluntarily under this program is presumed to be protected at the time the information is received. If the information is determined later to not qualify as protected, the submitting party has the opportunity to withdraw the information or it is destroyed, so as to avoid disclosure. However, the plain language of the statute makes clear this exemption only applies to information submitted to the DHS. It does not apply to records shared with the DoD.

Application

The underlying policy of FOIA favors disclosure; however, information disclosure can seriously impede collaboration. For the private sector, sharing information with the government exposes that information to release under FOIA. Trade secrets, sensitive information, and confidential client and organizational data could be released to the public. If the benefits of collaboration do not significantly outweigh the value of the confidential information that might be lost, the private sector will abstain from participation. From the government's side, release of records containing cyber risks could implicate mission security.

In addition, FOIA is administratively burdensome and procedurally uncertain. Neither party can predict with certainty the outcome of any FOIA request. If a private sector entity submits documents to the government, and even if the government denies a record request from a third party, that requester can appeal the denial by litigating the matter in court, subjecting the matter to judicial review. Typically, the record in question is kept confidential, but the possibility still exists that the document could be inadvertently "leaked." FOIA exemptions have little meaning if government employees fail to apply them correctly or mishandle records in a way that mistakenly makes them subject to disclosure. For example, if a government FOIA agent inadvertently or erroneously releases a document, the government may be able to physically retrieve the document, but the information in the document has been revealed, the economic

damage is done and the trust that must exist in a successful collaboration is destroyed. These examples provide explanation for the public sector's hesitancy to engage in information-sharing, FOIA's safeguards notwithstanding. Specific legislative action to address these FOIA concerns is discussed in the "Recommendations" section of this report.

FACA

Overview

The 1972 FACA (or the Act) was designed to "illuminate how agencies made decisions based on advice and recommendations from individuals outside of Government."¹⁷⁹ The Act responded to public concerns that advisory committees were "duplicative and inefficient, and otherwise lacking adequate controls or oversight" and did not adequately represent the public behind closed doors.¹⁸⁰ The Act was intended to control the growth and operation of the "numerous committees, board, commissions, councils, and similar groups which have been established to advise officers and agencies in the executive branch of the Federal Government."¹⁸¹

FACA applies to advisory committees established to advise the president or executive branch agencies and it provides for the management and oversight of these committees in order "to ensure impartial and relevant expertise."¹⁸² FACA also contains general guidelines for membership. It mandates that legislation establishing a committee must be "fairly balanced in terms of the points of view represented and the functions to be performed," and that "the

¹⁷⁹ "Twenty-Seventh Annual Report of the President on Federal Advisory Committees." Federal Interagency Databases Online. 13 Aug. 2009 <<http://fido.gov/facadbatabase/printedannualreports/1998-Twenty-Seventh%20Annual%20Report%20Of%20The%20President%20On%20Federal%20Advisory%20Committees.pdf>>.

¹⁸⁰ Smith, Stephanie. "Federal Advisory Committees: A Primer." CRS Report for Congress. 14 Jun. 2009. <<http://www.fas.org/sgp/crs/misc/RL30260.pdf>>.

¹⁸¹ 5 U.S.C. Appx. 1, § 2(a).

¹⁸² Smith, Stephanie. "Federal Advisory Committees: A Primer." CRS Report for Congress. 14 Jun. 2009. <<http://www.fas.org/sgp/crs/misc/RL30260.pdf>>.

commission's recommendations not be inappropriately influenced by the appointing authority or by any special interest."¹⁸³ The Act also does not apply to committees composed of full-time officers or employees of the federal government.¹⁸⁴

FACA's provisions governing access to committee meetings and records may have implications for cyber security collaboration. These provisions found in § 10 of FACA are similar to those of FOIA. However, FOIA's provisions apply to pre-existing documents while FACA's goal is to provide the public with access to meetings and materials generated for use by federal advisory committees.¹⁸⁵

Specifically, the requirements of § 10 of FACA mandate that the advice provided by advisory committees must be objective and open to the public.¹⁸⁶ To assure this openness, agencies must publish timely notes of planned meetings with the Federal Registrar.¹⁸⁷ FACA regulations require that all interested persons must be allowed to attend the meeting, appear before, or file statements with the advisory committee.¹⁸⁸ The "records, reports, transcripts, minutes, appendixes, working papers, drafts, studies, agenda, or other documents" of an advisory committee must be made available to the public.¹⁸⁹ Furthermore, detailed minutes of each meeting must be kept along with a record of those in attendance.¹⁹⁰ Because requests for the

¹⁸³ Smith, Stephanie. "Federal Advisory Committees: A Primer." CRS Report for Congress. 14 June 2009. <<http://www.fas.org/sgp/crs/misc/RL30260.pdf>>.

¹⁸⁴ "The Federal Advisory Committee Act." Federal Open Government Guide. 16 Jul. 2009. <<http://www.rcfp.org/fogg/index.php?i=faca>>.

¹⁸⁵ "Twenty-Seventh Annual Report of the President on Federal Advisory Committees." Federal Interagency Databases Online. 13 Aug. 2009 <<http://fido.gov/facadatabase/printedannualreports/1998-Twenty-Seventh%20Annual%20Report%20Of%20The%20President%20On%20Federal%20Advisory%20Committees.pdf>>.

¹⁸⁶ Smith, Stephanie. "Federal Advisory Committees: A Primer." CRS Report for Congress. 14 June 2009. <<http://www.fas.org/sgp/crs/misc/RL30260.pdf>>.

¹⁸⁷ This general rule applies "except where the President determines otherwise for reasons of national security, timely notice of each such meeting must be published in the Federal Register." 5 U.S.C.A. Appx 2, FACA § 10(a)(2).

¹⁸⁸ 5 U.S.C.A. Appx 2, FACA § 10(a)(3).

¹⁸⁹ 5 U.S.C.A. Appx 2, FACA § 10(b).

¹⁹⁰ 5 U.S.C.A. Appx 2, FACA § 10(c). However, closed deliberations may be held if one of the 10 conditions specified in the Government in the Sunshine Act are met. 5 U.S.C.A. Appx 2, FACA § 10(d). The committee must make a written determination in support of its decision that one of these conditions are met. 5 U.S.C.A. Appx 2, FACA § 10(d).

information under FACA are subject to the FOIA, requests must be made in accordance with the FOIA rules of the agency that supervises the operations of the advisory committee.¹⁹¹ As such, advisory committee records are subject to the same nine exemptions as FOIA.¹⁹²

Exemptions

FACA applies only to advisory committees which are defined as any group established by statute or utilized by the executive branch to obtain advice and recommendations.¹⁹³ Therefore, if a committee “is established by an agency head to obtain advice or recommendations for himself or other federal officers in the executive branch; and the committee is not composed wholly of full-time, or permanent part-time federal employees” the committee must abide by FACA’s requirements.¹⁹⁴ Notably, FACA “does not extend to a committee’s activities beyond its advice to the executive branch.”¹⁹⁵ FACA may also apply if an agency establishes the group or has a large share in controlling the group, such as setting the agenda or determining the membership.¹⁹⁶ Conversely, “if the committee is established and run by a non-federal individual or group it is not subject to FACA, even if federal employees are invited to participate.”¹⁹⁷

FACA does not apply when “the intent is to obtain information or viewpoints from individual attendees as opposed to advice, opinions or recommendations from the group acting in a

¹⁹¹ *National Sec. Archive v. Executive Office of the President*, 688 F. Supp. 29 (D.D.C. 1988), aff’d 909 F.2d 541 (D.C. Cir. 1990).

¹⁹² “The Federal Advisory Committee Act.” Federal Open Government Guide, 16 Jul. 2009 <<http://www.rcfp.org/fogg/index.php?i=faca>>.

¹⁹³ 5 U.S.C.A. Appx 2, FACA § 3(2). FACA applies if the committee “is established by an agency head to obtain advice or recommendations for himself or other federal officers in the executive branch; and the committee is not composed wholly of full-time, or permanent part-time federal employees.” “When if Federal Advisory Committee Act (FACA) Applicable?”

¹⁹⁴ “When is Federal Advisory Committee Act (FACA) Applicable?” U.S. General Services Administration, 29 Jul. 2009 <http://gsa.gov/Portal/gsa/ep/contentView.do?contentType=GSA_BASIC&contentId=10348>.

¹⁹⁵ “The Federal Open Government Guide.”

¹⁹⁶ Common Challenges for Partnerships, 29 June 2009. <<http://www.partnershipresourcecenter.org/resources/partnership-guide/chap8-3.html>>

¹⁹⁷ Common Challenges for Partnerships.

collective mode.”¹⁹⁸ A committee formed to monitor, conduct investigations, or perform activities other than providing advice does not fall under the purview of FACA even if it incidentally advises the agency.¹⁹⁹ Furthermore, “a group formed for some other purpose or to give advice to another entity that ends up giving advice to the agency also does not fall under FACA regulations.”²⁰⁰ Thus, as long as a committee does not directly provide advice to the executive branch leading to the establishment or implementation of a government policy, FACA is not implicated.²⁰¹

Application

FACA’s basic purpose is “to support the kind of open discussion and decision-making processes that occur in a collaborative environment.”²⁰² Accordingly, FACA has sometimes been seen as a barrier to collaboration.²⁰³ There is some fear on the part of the private sector that if they meet together with the government to discuss risks or vulnerabilities, those discussions might lead the government to establish or change policy. In such a case, the meetings and the information compiled at the meeting would have to be made public under FACA. However, as will be discussed in more detail in the Recommendation section, FACA concerns need not inhibit collaboration between the government and private sector. First, the information shared does not necessarily lead to the establishment or implementation of a governmental policy. Second, the voluntary nature of the collaborative membership and the lack of government control over collaboration agendas and operations argue against FACA application.

¹⁹⁸ “When is Federal Advisory Committee Act (FACA) Applicable?” U.S. General Services Administration, 29 Jul. 2009 <http://gsa.gov/Portal/gsa/ep/contentView.do?contentType=GSA_BASIC&contentId=10348>.

¹⁹⁹ “Common Challenges for Partnerships.” Partnership Guide, 29 Jun. 2009.

<<http://www.partnershipresourcecenter.org/resources/partnership-guide/chap8-3.html>>.

²⁰⁰ Common Challenges for Partnerships.

²⁰¹ FACA does not provide an explicit right to sue within the law itself, unlike FOIA or the Sunshine Act. It has been established that an individual who has been denied access to a transcript of an advisory committee meeting has standing to sue for its production under the Administrative Procedures Act. *Center for Auto Safety v. Tiemann*, 414 F. Supp. 215 (D.D.C. 1976).

²⁰² Common Challenges for Partnerships.

²⁰³ Common Challenges for Partnerships.

NON-LEGAL BARRIERS



Figure 4: The Real Issues are Non-Legal, as represented by the “fork in the road” sign

Some of the previously discussed laws do present actual legal barriers to collaboration; others are present barriers to collaboration because of the way the law is understood or could be applied.

While not minimizing these legal barriers, the team’s extensive outreach efforts to individuals in both sectors led to the conclusion that the major barriers to collaboration are non-legal. These include information-sharing, classification, security clearance processes, differing motivations, and cultures.

Information-Sharing

Many private sector representatives cited a lack of trust as inhibiting collaboration with the government. In particular, experts emphasized the one-way nature of information-sharing when dealing with government agencies. In other words, the government often requests information

from private sector industries without providing information of equal quality in return; reciprocity in information-sharing is often non-existent, according to private sector representatives. One interviewee from the private sector even expressed concern that information the company provided to the government went into a “black hole,”²⁰⁴ meaning the company was never told why the information was requested or the purpose it served.

Another complaint is that when the government does provide information, it is rarely timely or actionable. Sharing sensitive information with the government and getting little or no return constitutes a cost to the companies with little benefit. The private sector stated government has not presented a business case for information-sharing, meaning participating companies will have to invest time and resources without a clear financial return.

Compounding this issue is the constant worry in the private sector regarding the safety of the information submitted to the government. The risk of a leak of sensitive business information is something that could potentially cause lost revenue, diminished customer support, or even a business failure. Given this mistrust of the government, the private sector is often unwilling to engage in information-sharing.

Classification Issues

Outreach also identified over-classification of information as a barrier to the collaboration. The team heard the phrase “over-classification” in two different contexts: the volume of information classified by the government, and the level of classification assigned to the information. In 1995, former President Clinton issued Executive Order 12958, which updated the classification process as well as the handling of classified material. The same executive order established information

²⁰⁴ Bob Schlansker. Personal interview. 15 Jun. 2009.

is classified if it would be a threat to national security if released or made available to the public.²⁰⁵ In 2003, former President George W. Bush amended the classification procedure to expand the role of the Vice President and add “infrastructures” as a category of classifiable information.²⁰⁶ More recently, upon election, the Obama administration ordered a review of Executive Order 12958. Although the review is not yet complete, the current administration stated it aims to make the government more transparent.²⁰⁷ Preliminary recommendations of the current National Security Advisor include the creation of a National Declassification Center and “facilitat[ing] greater sharing of classified information among appropriate parties.”²⁰⁸ It is not clear how and when these initiatives will have substantial impact on government classification practices.

Businesses exhibited frustration with regard to classification practices when information on cyber attacks or breaches was shared with the government. An example that was discussed focused on information provided by a private sector entity which was then classified after it was in the hands of the government. When the company asked the government for insight about how the information was used or the purpose it served, the government refused to communicate about the issue because it had been classified. This was despite the fact that company was the original source of the information²⁰⁹. Likewise, some private sector individuals expressed fear that the quality of what the government would be able to provide within the collaboration would be affected by classification limitations.²¹⁰

²⁰⁵ Executive Order No. 12958.

²⁰⁶ Security Classification Policy and Procedure: E.O. 12958, as Amended. Congressional Research Service.

²⁰⁷ Security Classification Policy and Procedure: E.O. 12958, as Amended. Congressional Research Service.

²⁰⁸ President Barack H. Obama, “Memorandum of May 27, 2009—Classified Information and Controlled Unclassified Information,” p. 26277.

²⁰⁹ Eric Goldman. Personal Interview. 8 Jun. 2009.

²¹⁰ Tiffany Olson-Jones. Personal Interview. 15 Jun. 2009.

CULTURE

By its very nature, culture is stable and enduring and change does not occur quickly, so culture will be one of the most difficult barriers to overcome if the government wishes to collaborate with the private sector. Challenging as it may be, however, culture as a barrier must be understood in order to ensure collaboration success.

Each collaborator has its own specific culture with specific norms, values, motivations, priorities, and goals. These separate cultures often conflict, and attempting to merge the two for the purposes of collaboration has already proven to be an exceedingly difficult and complex undertaking. Also, the phenomenon of the unfettered or *laissez-faire* internet user promotes a culture of use that rarely emphasizes safety, secrecy, or smart online choices. The following sections provide further detail on these challenging cultural issues.

Differing Motivations

There is a significant difference between business and government motivations when each approaches the proverbial “table” to collaborate. In general, the DoD is motivated to protect the nation. This is made apparent by the DoD’s mission statement which “is to provide the military forces needed to deter war and to protect the security of our country.”²¹¹ The private sector is motivated by the business case. It focuses on economic gain, and the commitment and obligation it has to shareholders.²¹² In other words, the private sector seeks resources and investments that contribute to the business and its bottom line. Conversely, DoD interviewees rarely spoke in

²¹¹ “DefenseLINK Mission.” U.S. Department of Defense, 27 Jul. 2009 <<http://www.defenselink.mil/admin/about.html>>.

²¹² Vine, David. “Look After the Pennies.” *Working Life*. Apr. 2009. <www.AccountancyMagazine.com>.

economic terms. Both sectors recognized, however, it is important to protect cyberspace for reasons of both national and economic security.

While DoD personnel recognized that collaboration with the private sector is necessary, interviewees evidenced little understanding of the economic concerns of the private sector and often expressed uncertainty as how to move forward. It is clear from the team's interviews that barriers to collaboration, especially cultural barriers, can only be resolved through better understanding of and respect for each other's motivations.

Additional Cultural Issues

In addition to differing motivations, there are other cultural differences between the government and private sector that hinder collaboration. These cultural differences include citizenship issues, the speed of the decision-making cycle, consequences of information leaks, and cyber risk assessments. Each of these cultural issues will be addressed accordingly.

Citizenship Issues

A senior industry leader advised that the government needs to be prepared to work with individuals who are not U.S. citizens. Much of the private sector operates in an international market. Domestic corporations hire or conduct business with non-U.S. citizens, something the U.S. government is not willing or able to do in many cases.²¹³ Current government procedures limit non-citizen access to government facilities and information. To gain access, a company must go through a long and expensive process which does not guarantee security clearance for the non-U.S. citizen employee. Additionally, many of the best IT professionals, which include software developers, security specialists, and academics, are not U.S. citizens. The government's

²¹³ Tien, Lee and Peter Eckersley. "A Letter to the White House Cyber Security Review Team." *Electronic Frontier Foundation*. (undated).

stringent clearance requirements make it nearly impossible for these non-U.S. citizen IT professionals to collaborate with and access information from the government.

Speed of Decision-Making Cycle

As was previously discussed in the differing motivations section, the private sector is motivated by economic return while the government interviewees rarely spoke in economic terms. These differing motivations also can be seen in the relative speed of decision-making. Given the private sector's understanding that time is money, the private sector seeks to be the first to market. They must execute decisions quickly. Conversely, the government is bound by procedure, thus leading to much slower decision making process. This difference will hamper successful collaboration.

Consequences of Information Leaks

There are also differing consequences for both sectors when critical information is leaked or a breach of confidentiality occurs. The private sector risks losing profits and consumer or stakeholder confidence if confidential business information is leaked or accessed by third parties.²¹⁴ One private sector interviewee stated that an information leak can be so detrimental to a company that it can lead to bankruptcy.²¹⁵ Additionally, supply chain threats are always real, as any link in the chain being disabled can fundamentally disrupt business activities.²¹⁶ While a government information leak can have negative effects on things such as its mission success, the government does not face lost profits or bankruptcy. As one interviewee stated, the government

²¹⁴ Wybourne, Martin N., Martha F. Austin, and Charles C. Palmer. "National Cyber Security Research and Development Challenges Related to Economics, Physical Infrastructure, and Human Behavior." *An Industry, Academic, and Government Perspective*. Institute for Information Infrastructure Protection (I3P), 2009.

²¹⁵ Weeks, Jeffery. Personal Interview. 02 Jul. 2009.

²¹⁶ Wybourne, Martin N., Martha F. Austin, and Charles C. Palmer. "National Cyber Security Research and Development Challenges Related to Economics, Physical Infrastructure, and Human Behavior." *An Industry, Academic, and Government Perspective*. Institute for Information Infrastructure Protection (I3P), 2009.

employee responsible for the leak might simply get a slap on the wrist. It is important for the government to understand the private sector's concerns about information protection.

Evaluating Cyber Threats

Another cultural difference between the government and private sector is that both sectors evaluate cyber threats differently. The government interviewees stated that the private sector does not realize the threats that exist in cyberspace and that they will not take such threats seriously until a cyber catastrophe occurs. In contrast, the private sector experts stated that the government miscalculates cyber threats by focusing on the wrong issues. In order to create a successful collaboration, the two sectors must have a common understanding of what constitutes a cyber threat and how to best respond to various types of threats. Cyber threats vary from one sector to another and thus a one-size-fits-all approach will not work to secure the cyber domain.

User Culture

The Institute for Information Infrastructure Protection (I3P) noted in its 2009 publication on National Cyber Security, "[Cyber] security depends not only on technology, but also on the awareness, knowledge, and intentions of the employees, customers, and others using information-based systems and networks."²¹⁷ Thus, the human aspect of cyber protection and defense cannot be underestimated. The same article also illustrates the danger of common user culture, stating the pervasiveness of internet and technology in the everyday lives of American citizens creates a feeling of trust and security that can result in unintended consequences.²¹⁸

²¹⁷ Wybourne, Martin N., Martha F. Austin, and Charles C. Palmer. "National Cyber Security Research and Development Challenges Related to Economics, Physical Infrastructure, and Human Behavior." *An Industry, Academic, and Government Perspective*. Institute for Information Infrastructure Protection (I3P), 2009.

²¹⁸ Wybourne, Martin N.

For example, online shopping, banking, and social networking, all promote providing sensitive personally identifiable information. Whether it be through entering a credit card number at an online auction, providing a bank account number to access a checking account, or posting a cellular phone number and home address on a blog, people are constantly jeopardizing their personal safety online.²¹⁹ The numbers of people conducting such activities online is already quite staggering and is increasing daily. In fact, the Pew Internet and American Life Project, headquartered in Washington D.C. found that in 2005 nearly 50% of all American internet users made use of online banking services.²²⁰

Additionally, approximately one third of American adults using the internet have a profile on an online social networking site, but this is only half the amount of American teens that have a profile.²²¹ While 58% of the adults using social networking sites restrict access to certain users, a mere 21% of teens restrict access to the same information.²²² This research indicates that a growing number of individuals are providing unsafe information online, and the younger generations are growing up in a culture where these practices are acceptable and commonplace. As the future employees in the American private sector and government, the growing *laissez-faire* attitude of user culture is a dangerous prospect for the protection of sensitive proprietary information and national security alike.

Even more startling are the numbers of people using the internet for non-work related purposes at work. One study found the average employee spends between 30 minutes and 3 hours of on-

²¹⁹ Wybourne, Martin N., Martha F. Austin, and Charles C. Palmer. "National Cyber Security Research and Development Challenges Related to Economics, Physical Infrastructure, and Human Behavior." *An Industry, Academic, and Government Perspective*. Institute for Information Infrastructure Protection (I3P), 2009.

²²⁰ Fox, Susannah and Jean Beier. "Online Banking 2006: Surfing to the Bank." The Pew Internet and American Life Project. 2006. <http://www.pewinternet.org/~media/Files/Reports/2006/PIP_Online_Banking_2006.pdf.pdf>.

²²¹ Lenhart, Amanda. "Adults and Social Network Sites." The Pew Internet and American Life Project. January 2009.

<http://www.pewinternet.org/~media/Files/Reports/2009/PIP_Adult_social_networking_data_memo_FINAL.pdf.pdf>.

²²² Lenhart, Amanda.

the-clock time checking social networking sites, shopping, or simply surfing the web for entertainment purposes, resulting in decreased productivity and losses of up to \$12 billion annually.²²³ Just as damaging as the loss of productivity and profits is the threat of spyware, phishing, and hacking that can come as a result of unsafe internet use at work.²²⁴ Often, the use of a social networking site, instant messenger service, auction site, peer-to-peer site, or any other site in which an individual is connected to other users, leaves the door wide open for intruders and malicious users. A breach of a personal computer at home can be damaging to a singular individual, but a breach of a corporate or government network can threaten the entire company, critical infrastructure, or even national security.

General Chilton recognized the need for a cultural change within the DoD when at the 2009 Cyber Symposium he stated “We have to transition from a culture of convenience to a culture of responsibility.”²²⁵ Similarly, the 60-day Cyberspace Policy Review also recognized the importance of a public culture shift, saying “The U.S. needs to conduct a national dialogue on cyber security to develop more public awareness of threats and risks...in a way that the American people can appreciate the need for action.” Recommendations on how to address cultural issues appear in the Recommendations section of this report.²²⁶

²²³ Kelleher, David. “Social Networking at Work: Fear Not Facebook and Myspace.” 23 Feb. 2009. <<http://www.itworld.com/internet/63062/social-networking-work-fear-not-facebook-myspace>>.

²²⁴ Kelleher, David.

²²⁵ General Chilton, Kevin P. 2009 Cyberspace Symposium. 7 Apr. 2009. <http://www.stratcom.mil/speeches/23/2009_Cyberspace_Symposium>.

²²⁶ *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.*”

LEGAL RECOMMENDATIONS

The team identified several statutes that created barriers to collaboration. Legal recommendations to address those statutory barriers are discussed below.

FISA

FISA is a means for the government to use telecoms to access customer information. It discourages collaboration between the government and companies as many customers do not trust the government will handle their information correctly. The latest amendments to FISA have proven to be contentious as evidenced by lawsuits challenging the constitutionality of the legislation. The team has two recommendations for overcoming FISA concerns.

While FISA does not directly hinder collaboration, the public's perception of FISA affects the relationship between the government and private sector. Therefore, a statutory change is necessary. One FISA change was recently introduced by Senator Arlen Specter. Senate Bill 876 which would allow for civil suits by substituting the government for the information provider.²²⁷ This change to the Act may calm concerns that under current immunity provisions in FISA U.S. citizens are unable to seek redress for infringement of their civil liberties.

Additionally, the team believes that strengthening the current legal requirement for obtaining a FISA warrant might also aid in altering public perception of FISA. The provision of FISA authorizing electronic surveillance requires a lesser showing than the traditional probable cause

²²⁷ S. Bill 876. The Library of Congress. Introduced by Senator Arlen Specter. 23 Apr. 2009. 13 Aug. 2009. <<http://thomas.loc.gov/cgi-bin/bdquery/D?d111:1:/temp/~bdyjyp:@@L&summ2=m&/bss/111search.html>>.

standard for the government to obtain a warrant for electronic surveillance in other contexts.²²⁸

Making the requirements to obtain a FISA warrant as stringent as those for obtaining a warrant for purely domestic surveillance may alleviate the public's concern that FISA violates their civil liberties. However, altering legislation, especially legislation as controversial as FISA, is typically a time consuming process with no guaranteed outcome. Also, any FISA amendment must balance and address the public privacy concerns with facilitating the government's ability to prevent attacks on the Homeland.

Regardless of the legislative changes considered, the government's historical use of FISA is a barrier to collaboration because of public fears of government involvement in their personal communications. In a nation that values autonomy and fosters a healthy fear of government involvement, it is understandable that FISA would raise suspicions. Alleviating the concerns of U.S. citizens may be achieved by educating the public on the goal of FISA while providing more transparency to the government's use of the power granted to it. Finally, there should be consideration given to standardized language in cyber services contracts discussing in plain English what FISA is, the procedural requirements for the government to use FISA, and the rights of customers under the statute.

²²⁸Kennel, John R. and Jane Lehman. "Electronic Surveillance; Wiretapping." American Jurisprudence, Second Edition. May 2009. 68 Am. Jur. 2d Searches and Seizures § 348. 13 Aug. 2009.
<https://web2.westlaw.com/result/default.wl?fmqv=s&sv=Split&vr=2.0&sskey=CLID_SSSA89245565710188&rs=slss1.0&utid=2&action=Search&db=AMJUR%2cCJS&eq=search&fn=_top&srch=TRUE&rp=%2fSearch%2fdefault.wl&cfid=1&rlt=CLID_QRYRLT79652575710188&rltdb=CLID_DB99230565710188&origin=Search&mt=LawSchoolPractitioner&service=Search&qquery=FISA+standard&method=WIN>.

FOIA

As discussed in the FOIA section, the private sector expressed serious concerns that information they share with the government in any cyber collaboration would be subject to release under FOIA. While Exemption Four could arguably protect this information as CBI, there remain uncertainties in the application of the Exemptions and with FOIA processes.

The best solution would be for the government to seek a new FOIA exemption statute similar to the one granted to DHS that is focused on the protection and defense of cyberspace. Pending legislative action on such a new FOIA exemption, Executive Order 13292 could be amended to allow for the inclusion of information relating to e-threats and vulnerabilities within the definition of “national security” for purposes of Exemption One protection. This would allow for the classification of cyber information shared with the government. However, classification of information brings problems with the handling and further sharing of information. These problems must be weighed against the protections that a new classification category would grant.

Antitrust

When “virtually any concerted action among two or more entities may be susceptible to Section 1 challenge, provided that it is shown to have the requisite actual or threatened anticompetitive impact and to meet certain threshold procedural and substantive requirements” companies are rightfully skittish for not wanting to engage in anything that appears to give the impression of an agreement or information-sharing that can impact the market.²²⁹

²²⁹ Holmes, William C. Antitrust Law Handbook. 2008-2009 ed. Thomson Reuters/West, 2008. pg 101.

After meeting with an antitrust expert, the team concludes that antitrust law should not be a barrier that cannot be overcome to prevent information-sharing between the private sector and the government.²³⁰ An antitrust exemption specifically addressing information-sharing for the purpose of securing networks and infrastructure, and thereby increasing cyber security for the nation, would provide the best assurance to companies that they will not violate antitrust laws. While current antitrust law would permit collaboration between companies as long as it does not unreasonably restrict trade, companies are obviously unwilling to take any risks and will avoid meeting with their competitors altogether.

Such an exemption would need to be passed by Congress and apply specifically to § 1 of the Sherman Act. The exemption would create an information-sharing safe harbor for the purpose of protecting and defending cyberspace. As long as agreements and collaboration among competitors was limited to cyber security information, companies would not have to concern themselves with violating the Sherman Act. Prosecution of *per se* or rule of reason violations would not be an issue as this type of collaboration would be clearly allowed by statute.

The team learned of a similar exemption currently in statute that permits information in the insurance industry.

Getting a legislative change through Congress often takes years, but protecting cyberspace is a current national concern. For this reason, an agency ruling could be a more attractive option. The DoJ could write an approval letter that would assure companies they would not be investigated or sued for working with their competitors as long as the activity was information-sharing and was limited to protecting cyberspace. The Antitrust Division of the DoJ has the expertise and

²³⁰ John Lenich. Personal Interview. 1 Aug. 2009.

authority to write such a letter.²³¹ The Department partnered with the Federal Trade Commission (FTC) to issue “Antitrust Guidelines for Collaborations Among Competitors” in 2000 and the letter could be based on many of the principles and legal concerns espoused in the Guidelines.²³² A joint effort between the Antitrust Division of the DoJ and the FTC to produce an approval letter would also provide a good faith effort by the government to assuage the antitrust concerns voiced by the private sector for information-sharing.

By creating a statutory safe haven for cyber security information-sharing via legislation or assuring no prosecution for cyber information-sharing through a DoJ approval letter, the government can assure companies that working with their competitors towards cyber security will not violate antitrust laws. Such assurance will show the private sector the government is sincere in its desire to collaborate with the private sector to protect and defend cyberspace.

²³¹ “The President’s National Security Telecommunications Advisory Committee: Executive Summary.” NSTAC XXV Issue Review: 20th Anniversary Edition 1982-2002, “Executive Summary,” Aug. 2002 at A10-14 (referencing Letter to Lr. Gen. William Hilsman, Manager, National Communications Systems, from William F. Baxter, Assistant Attorney General, Antitrust Division, June 1, 1983). Pg 123. As cited by Westby, Jody R, ed. International Guide to Cyber Security. Chicago: ABA, 2004.

²³² Federal Trade Commission and the U.S. Department of Justice. Guidelines for Collaboration Among Competitors. 2000. <<http://www.ftc.gov/os/2000/04/ftcdojguidelines.pdf>>.

NON-LEGAL RECOMMENDATIONS

Develop a Common Language

Developing a common language would facilitate communication between collaborating parties.

This could be as simple as creating shared definitions for key terms. Currently, the private sector and the government communicate through languages referred to as “private sector speak” and “government speak.” These different dialects include differing terminology for congruent definitions and an abundance of abbreviations that may confuse the other sector. Once a common lexicon has been created, there will be a reduction in misinterpretations of data and miscommunication between the government and private sector

Decrease Over-Classification

Limiting the amount of classification of cyber related information encourages collaboration because it opens the door to more two-way information-sharing rather than the “black hole” that currently exists. Confidential information shared with the government by the private sector should still be treated as sensitive and be protected against any release to the public. More open communication aids both the government and the private sector by encouraging true collaboration resulting in better ways to predict and respond to future threats. Therefore, the government should review its national security classification procedures and decrease the amount of over-classification, both in volume and degree.

Change Security Clearance Protocol

Non-U.S. citizens cannot qualify for security clearance except in the most limited circumstances.²³³ Several members of the private sector, however, noted they have a number of non-citizen employees who could make the most beneficial use of government classified information. While non-citizens can qualify for Limited Access Authorizations (LAAs), this clearance is costly and time consuming for the company. Being granted an LAA requires proving that a qualified citizen cannot be hired in sufficient time.²³⁴ Even a flawless application will not guarantee a grant of an LAA for the non-U.S. citizen employee. The government could revise security protocols to allow for more security clearances to be granted for non-U.S. citizens working on cyber security or information-sharing for their companies. Allowing the most qualified employees to be involved in cyber security will enhance collaboration efficiency and demonstrate to the private sector that the government is committed to a successful collaboration.

Begin Collaboration with Bilateral Agreements

Interviewees from the government and private sector stressed the importance of personal working relationships when bridging the gap between them. Many of the differences between the business culture and the government culture are more easily overcome when collaboration is on a personal level. It is important for both sides to share their expectations and concerns in the area of cyber threats and information-sharing. A bilateral meeting or collaboration with the government eliminates all antitrust concerns. In this setting, both the government and the private

²³³ Defense Security Service. International Programs: Limited Access Authorizations (LAAs) for Non-U.S. Citizens. <<https://www.dss.mil/GW/ShowBinary/DSS/isp/international/laa.html>>. 13 Aug. 2009.

²³⁴ Defense Security Service.

sector can benefit from mutual information-sharing and develop trust for one another; this could be a promising start for a long-term collaborative relationship.

Shift Culture through Training and Education

As described in the Culture section of this report, culture is a challenging barrier to overcome. Extensive outreach efforts and research indicated increased training and education are some of the most effective means of addressing business, government, and user culture issues.

Shifting Business and Government Culture through Training

During the 2009 Cyberspace Symposium, General Chilton stressed “the importance of training and ensuring each service member recognizes the potential consequences of their actions.”²³⁵

Based on the General’s speech, the team recommends business and government culture be shifted to focus more heavily on smart, safe, and secure network use. Regardless of differing cultural motivations, priorities, and goals, it is the responsibility of each corporation, institution, agency, and department to protect cyberspace by providing proper training. While the government already provides training in cyber security, outreach experts stated the government fails to enforce the rules its training is based on. As a result, there is a tendency for government employees not to afford cyber security the proper priority. Therefore, training should be better enforced with greater consequences for failing to comply. Additionally, as new cyber threats emerge, training programs should be updated to reflect and address these threats. Although it may seem like a large, costly, and time consuming effort, not doing so could have extraordinarily detrimental effects.

²³⁵ General Chilton, Kevin P. 2009 Cyberspace Symposium. 7 Apr. 2009.
<http://www.stratcom.mil/speeches/23/2009_Cyberspace_Symposium>.

Shifting User Culture through Education

When the U.S. realized it had a serious problem with youth drug abuse, a group of educators, law enforcement officials, parents, and community leaders gathered together to create the Drug Abuse Resistance Education program, or D.A.R.E.²³⁶ The mission of the D.A.R.E program is to “provide children with the information and skills they need to live drug and violence free lives.”²³⁷ In most cases, D.A.R.E. takes place in the children’s classrooms and is now being implemented in 75 % of U.S. schools and over 40 countries around the world.²³⁸ The program starts at kindergarten and continues through 12th grade, with the underlying assumption that minds can be molded and culture can be shifted if started at an early age.²³⁹

The team recommends instituting a public program for cyber safety education using the D.A.R.E. program as a model. Cyber education should start young and continue to evolve based on age and computer sophistication. The program should also take place in the school setting so it is standardized and enforceable. Given the pervasive use of social networking among teenagers, a portion of the program should be tailored specifically to safe usages of these social sites, including the creation and use of secure passwords and what types of information is appropriate to post online. Because many schools around the nation already have computer classes for keyboarding, and programming, a section on internet safety could easily be included.

²³⁶ “The D.A.R.E. Mission.” D.A.R.E. America. <www.dare.com/home/THEDAREMISSION.asp>.

²³⁷ “The D.A.R.E. Mission.”

²³⁸ “About D.A.R.E.” D.A.R.E. America. <http://www.dare.com/home/about_dare.asp>.

²³⁹ “About D.A.R.E.”

ISHARE – A NEW APPROACH TO PARTNERING

In order to protect and defend cyberspace, the team recommends creating ISHARE, a non-profit entity to address e-threats.²⁴⁰ ISHARE, or Information Sharing to Help America Recognize and Respond to E-Threats, would encourage collaboration between the government and private sector by creating a secure and easily accessible forum for information-sharing. ISHARE would not be a policy-generating body, but be a real-time information-sharing mechanism based on emerging technology such as Web 2.0.

ISHARE would create a user-friendly website for instant, non-attributed information-sharing. More specifically, ISHARE would be structured similar to a discussion board in which members of the website post real-time information regarding new threats or solutions to existing threats useful to the government and other ISHARE members. In return, the government would post information that it thinks will be helpful to ISHARE members. This timely reciprocal information exchange is crucial to protecting and defending cyberspace as both sides would have a more complete situational awareness of vulnerabilities.

ISHARE would be funded by the federal government, perhaps through a cooperative agreement, and would be administered by a board consisting of representatives from private industry, academia, and government. ISHARE would not be a military-run or private sector-run entity, but would employ cross-sectional experts to render independent advice on the operations of the ISHARE website. To reinforce the independence of ISHARE from the government, the chairperson of the board of directors should be a member of the private sector selected on a

²⁴⁰ E-Threats are defined as any type of threat that affects the functionality and security of cyberspace, as defined by the team.

rotating basis.²⁴¹ ISHARE could be housed at an academic institution to integrate the capabilities of experts outside of government and private industry.

ISHARE should start with a small pilot program consisting of members from a variety of critical infrastructure industries to beta test the online sharing technology, develop the trust necessary for information-sharing, and ensure efficiency of the organizational operating rules. Expanded ISHARE membership would be limited to companies based in the U.S. as ISHARE should focus on domestic interests and serve as a component of national security.

As indicated in Figure 5, ISHARE would be a new approach to information-sharing and collaboration. Although there are existing information-sharing programs such as Computer Emergency Response Team (CERT), Information-sharing and Analysis Center (ISAC), and InfraGard, these programs have yet to create a truly successful collaboration. Each of these existing approaches has problems ISHARE would address. For example, several private sector representatives noted that CERT focuses on past threats instead of future issues. Conversely, ISHARE offers postings of real-time threats as they arise. ISACs are funded by private industry companies allowing for free riders that receive the benefit of the information without contributing to the program. ISHARE on the other hand, while funded by the government, would require all participants to contribute information equally and the benefit would be shared. The InfraGard approach consists mostly of untimely, open-source information, which is often not helpful for real-time threats. With real-time postings, ISHARE members will be able to act immediately on information received without the delay of information going to a government source to be analyzed and filtered before being returned to the user. Figure 5 summarizes the differences between ISHARE and existing organizational approaches.

²⁴¹ The team recognizes that even having government employees serve as members of the board may raise ethics issues. An alternative approach would be to have government representatives serve in an ex-office non-voting status.

	CERT	ISAC	InfraGard
Problems	<ul style="list-style-type: none"> • Looks at past threats, not future issues and attack management • Untimely information • Not exclusive to information-sharing • Open membership 	<ul style="list-style-type: none"> • Funded by private sector leading to free riders • Connection to Federal agencies create FOIA concerns 	<ul style="list-style-type: none"> • Open source • Untimely information • Not actionable • Administered by FBI
ISHARE is different	<ul style="list-style-type: none"> • Prevent future events • Provides real-time information • Exclusive to information-sharing • Limited membership 	<ul style="list-style-type: none"> • Government funded • Moderated by third party 	<ul style="list-style-type: none"> • Secure information voluntarily provided • Mitigate existing threats • Not tied to one particular Federal agency

Figure 5: Summary of Differences Between Existing Programs and ISHARE

ISHARE AS A NON-PROFIT ENTITY

Cost and legitimacy are two of the more pragmatic reasons why ISHARE should be created as a non-profit agency. To receive non-profit status, ISHARE must fit into one of the statutory non-profit organization categories. Nonprofit status underscores the educational and non-commercial intent of the organization and helps protect members from some legal challenges such as those based on antitrust concerns.

In addition to having lower overhead costs because of the federal income tax exemption, giving ISHARE a non-profit status adds legitimacy. If members of the private sector are convinced that ISHARE is not profiting from its information-sharing service and is simply facilitating the flow of information between government and industry, they are more likely to participate.²⁴²

Conversely, if ISHARE profited from the information-sharing when the individual company volunteered the information that company will be less inclined to participate.

Non-profit organizations are often referred to as 501(c) organizations because their special tax treatment is detailed in § 501(c) of the United States Internal Revenue Code.²⁴³ The section provides for exemption from the federal income tax for organizations that fit into one of 28 categories. ISHARE could qualify under one of two categories, §501(c) (1) and (6).

The first category, § 501(c)(1) exempts organizations that were created pursuant to an act of Congress.²⁴⁴ Although ISHARE is not currently exempted by part (B) of § 501(c)(1), congressional action to include ISHARE in this provision could be pursued.

²⁴² Professor Bill Lyons, Nebraska College of Law. Personal interview, July 27, 2009.

²⁴³ 26 U.S.C § 501(c)

²⁴⁴ 26 U.S.C § 501(c)(1)

ISHARE as a organization that facilitates information-sharing among businesses for the benefit of those businesses could qualify in § 501(c)(6). This category exempts “Business leagues, chambers of commerce, real-estate boards, boards of trade...not organized for profit and no part of the net earnings of which inures to the benefit of any private shareholder or individual.”²⁴⁵ ISHARE would not generate any profits; the benefits of the organization would come from in increased efficiency and security for members of ISHARE.

ISHARE and Legal and Non-Legal Barriers

As discussed above, the ISHARE concept is meant to address shortfalls in several existing approaches. In addition, the team believes the ISHARE organization can also alleviate many of the legal and non-legal concerns expressed during outreach.

Legal

Patriot Act/ FISA

The Patriot Act and FISA describe how the government can intercept telephone and electronic communications. Because ISHARE is not a government run or law enforcement organization, the Patriot Act and FISA concerns discussed in this report should not inhibit collaboration. ISHARE would not need to collect cyber and electronic content information through searches. It would use voluntarily provided information from its members.

Procurement Law and FAR regulations

Procurement Law and the implementing FAR regulations dictate how the government acquire goods and services. By placing the ISHARE organization outside government control,

²⁴⁵ 26 U.S.C § 501(c)(6)

government procurement laws and regulations should not affect this collaboration. The team recommends the cooperative agreement to establish ISHARE be awarded to a university or other competent non-profit organization. Under a cooperative agreement the party receiving federal funds may have to comply with certain FAR-like requirements, but the collaborating members would not. In addition, to ease private sector worries, the collaborating parties could agree the shared information would not be disseminated to government procurement organizations.

FOIA

FOIA concerns public access to government records. A government record is a record under the control of a government agency. ISHARE documents would not be under government control. Some might argue that the information shared by the government with collaborators in ISHARE is subject to FOIA to the extent it was first created and controlled by the government. If that were found to be so, the government would have the normal procedures and exemptions available to it to respond to a FOIA request for government information. Even if government generated information were subject to FOIA, private sector information would not.

FACA

FACA provides public access to committees established or used by the government to set policy. ISHARE is not a committee nor is it policy setting body. It would not recommend changes to government cyber security laws, regulations or practices.

Antitrust

ISHARE would be open to any U.S. private sector company that agrees to the business rules of the organization; therefore, no boycott claim can be made. ISHARE private sector members will

likely be competitors in the cyber markets. However, these competitors will not be meeting to fix prices, establish standards or divide market share. Their interactions would be limited to identifying and sharing cyber security issues.

Non-Legal

Cultural and differing motivations

As the research established the non-legal barriers, especially the differing cultures and motivations of the parties, present challenges to successful collaboration. ISHARE offers an excellent forum for addressing those barriers. As was discussed, changing culture is extremely difficult and time consuming. ISHARE parties will have the opportunity to develop a new culture, one based on the two existing cultures but unique to the collaboration. In the same way, the ISHARE forum would allow the parties to develop an appreciation for each collaborator's motivation. As understanding grows, so will the trust. Over a relatively short time ISHARE should generate an atmosphere that not only facilitates collaboration but encourages the type of out of the box thinking that will be necessary to solve the ever evolving challenge of cyber security.

FUTURE RESEARCH

International collaboration and the role of academia are two major topics that should be the focus of future research. Due to time constraints, the team focused its research primarily on domestic legal and non-legal issues and recommendations. However, international issues are an important consideration because cyberspace does not respect national borders. Differing laws, cultures, and the assortment of international organizations, treaties, and agreements are considerations in fostering successful collaboration across nations.

There is little established international law regarding cyberspace. Instead, international cyberspace frameworks and understanding are currently created through political agreements, allowing for countries to establish international collaboration and agreement on how to approach cyberspace with their own sets of laws to which they must adhere. For example, privacy laws of the U.S. conflict with those of the European Union, even though both bodies represent Western nations with democratic traditions.²⁴⁶ The European Union's privacy laws grant greater deference to governments while U.S. privacy laws are slanted in favor of individual rights. Understandably, each nation would seek to have its own legal and cultural position guide response to any cyber attacks within its borders or affecting its citizens.

Additionally, developing nations for whom cyberspace security is not a priority must also be considered. The challenge regarding these nations is how to induce the nation to prioritize cyber security while ensuring the development of other, equally important areas of the nation's infrastructure, such as housing, transportation, or healthcare are not disadvantaged.

²⁴⁶ Sullivan, Bob. "'La difference' is stark in EU, U.S. privacy laws: EU citizens well protected against corporate intrusion, but red tape is thick." *Msnbc*. N.p., 19 Oct. 2006. Web. 10 Aug. 2009. <<http://www.msnbc.msn.com//>>.

The same discussion regarding international legal obstacles applies with equal force to international cultural issues. Laws are effective when they embody a nation's values. A nation's culture will influence how it approaches cyberspace. These differences in culture also lead to differing motivations and expectations. For example, the U.S. may be motivated to protect and defend cyberspace in order to properly secure critical infrastructure and national security.

However, a developing country may not have these same motivations. Outreach conducted with individuals who have international cyberspace expertise analogized the situation to Maslow's Hierarchy of Needs. One country may be unable or unwilling to expend resources on the security of cyberspace when concerns such as food, water, or public safety are much bigger, more pressing issues.

Moreover, outreach indicated that other countries may derive benefit from lax or inadequate U.S. cyber security. One FBI Special Agent explained that government officials in developing countries often ignore cyber attacks initiated by their citizens if those attacks provide direct or indirect economic benefits to their country. Specifically, he mentioned that certain aspects of the Nigerian economy rely on credit card fraud, identity theft, and stealing money through various cyber attack methods.

Existing frameworks like international organizations and agreements, can offer guidance when dealing with legal and cultural differences between nations. Outreach cited the North Atlantic Treaty Organization (NATO), World Trade Organization (WTO), International Police (INTERPOL), United Nations (UN), Group of Eight (G8), Organization of American States (OAS), Council of Europe, and Five Eyes as key international organizations. However, many of these organizations simply create guidelines that document how each member should act and policies that should be abided, but they tend to lack overall enforcement power. A senior

industry leader of a major computer software company stated that INTERPOL and the WTO are the only organizations that possess any enforcement power.²⁴⁷ For example, the OAS may bring international entities to the table to openly discuss problems, but at the end of the day, each country has only diplomatic strategies and bargaining tools to address international cyber issues. These strategies include pulling diplomats out of the foreign countries, enacting embargos or other trade strategies such as international sales taxes, sanctioning the country, or creating and utilizing extradition treaties.

However, there are pros and cons to each of these strategies. Pulling diplomats out of a country eliminates communication, and without communication, a collaborative solution is not possible. Establishing an embargo or other trade strategies has the ability to negatively affect the economy of the country in question, but also the country that initiates the changes in trade. Sanctioning a country through an international forum is not always helpful. If the country in question has already deliberately violated international policies and rejected reform, they may also refuse to continue to participate in the international organization from which it has been sanctioned. For example, North Korea ignored sanctions from the UN and even responded by threatening future sanctions issued by the UN with “corresponding self-defense measures” and the use of nuclear missiles.²⁴⁸ Extradition treaties can be used if the source of a cyber attack can be attributed. However, the U.S. does not have extradition treaties with all nations. In fact, the U.S. does not have extradition treaties with either China or Russia, two countries from which cyber attacks are launched.²⁴⁹ Understanding these complex international issues requires more study.

²⁴⁷ David Aucsmith. Personal Interview. 14 July 2009.

²⁴⁸ Lederer, Edith M. “North Korea Sanctions Unanimously Expanded By U.N. Security Council.” *The Huffington Post*. N.p., 12 Jun. 2009. Web. 7 Aug. 2009. <http://www.huffingtonpost.com///korea-sanctions-una_n_214885.html>.

²⁴⁹ “United States Extradition Treaties.” *Nation Master*. N.p., n.d. Web. 10 Aug. 2009. <http://www.nationmaster.com/_uni_sta_ext_tre_cit-united-states-extradition-treaties-citation>.

Future research should also focus on academia. A professor of Criminal Law and Cybercrimes noted that because academia is part of the private sector, it shares many of the sector's concerns, but also brings a unique perspective to forming an effective collaboration.²⁵⁰ Academic culture is significantly different from that of the private sector or the government. Academics operate in an open environment and are required to publish their research and findings. The concept of peer review encourages academicians to openly and candidly discuss their subject knowledge.

Academia can operate as an “honest broker” between the government and private sector and can promote actionable solutions for collaboration barriers. Academics can hold seminars to discuss the legal and cultural issues and create training and educational programs. Lieutenant Colonel Darren Huskisson (USAF) indicated that many cyberspace issues could benefit with help from academics, as academics have time and resources to do research that may not be possible for the government or private industry.²⁵¹ A Professor of Communication Technology, Law and Policy stated that academics may be able to help the government prevent cyber attacks as they sometimes foresee emerging technical issues, but often do not have established relations with the government to share these insights. However, academics have also expressed mistrust of both the private sector and the government. Many academics disagree with the means and goals of the DoD and private industry. For example, when the DoD discusses the use of the internet as a weapon system, many in academia object.

Academics can also help address a common concern voiced by many outreach participants—the lack of qualified IT security professionals. A significant number of IT students graduating from U.S. schools are non-U.S. citizens. Not only do these IT security employees have less access to government information, but many are choosing to obtain their degree in the U.S. and then return

²⁵⁰ Susan Brenner. Personal Interview. 03 June 2009.

²⁵¹ Lt. Col. Darrin Huskisson. Personal Interview. 28 Jun. 2009.

to their home country. The future study should focus on quality, quantity, and retention of IT professionals as part of a larger cyber-security enterprise.

CONCLUSION

The team's work focused on answering the research question regarding the legal and non-legal barriers that need to be addressed if the DoD collaborates with the private sector to protect and defend cyberspace. The research indentified a limited number of statutes that outreach experts indicated as barriers. In addition, the team found that the non-legal barriers of culture and differing motivations were equally, if not more significant to information-sharing and collaboration.

The team has made recommendations as to how to amend or interpret statutes perceived as barriers. Other legal concerns could be addressed through education, dialogue, and discussions, particularly on the bilateral level between private sector and government lawyers. Training and education are also primary methods of addressing non-legal barriers. Recommendations in the area are geared toward enhancing government and private industry training to keep it up to date and enforceable. Additionally, a cyber security education training program is recommended to teach the next generation of government officials and private industry leaders how to safely and properly behave in cyberspace. Additional recommendations include adjusting security protocols and classification measures.

The team also recommended an organizational solution; the establishment of an on-going, trusted, reciprocal collaboration between sectors via the ISHARE model. The team believes this model addresses many of the legal and non-legal barriers to collaboration. Finally, the team made specific recommendations for future research

BIBLIOGRAPHY

- 5 U.S.C.A. Appx 2, FACA § 3(2).
- 5 U.S.C. § 552b (b).
- 5 U.S.C. § 552(b)(3).
- 5 U.S.C. § 552(b)(4).
- 5 U.S.C. § 552b (c).
- 5 U.S.C. § 552b (c)(2).
- 5 U.S.C. §552(f)(2).
- 5 U.S.C. Appx 1, § 2 (a).
- 5 U.S.C. Appx 2, FACA § 3 (2).
- 5 U.S.C. Appx 2, FACA § 10 (a)(2).
- 5 U.S.C. Appx 2, FACA § 10 (a)(3).
- 5 U.S.C. Appx 2, FACA § 10 (b).
- 5 U.S.C. Appx 2, FACA § 10 (c).
- 5 U.S.C. Appx 2, FACA § 10 (d).
- 10 U.S.C. § 371.
- 10 U.S.C. § 371-375.
- 15 U.S.C. § 1.
- 15 U.S.C. § 1, 2.
- 15 U.S.C. § 15(a).
- 15 U.S.C § 15(b)(1).
- 15 U.S.C § 15(c).
- 17 U.S.C. § 101.
- 17 U.S.C. 102(b).
- 17 U.S.C. § 106.
- 18 U.S.C. § 1385.
- 18 U.S.C. §§ 2510-2522.
- 26 U.S.C § 501(c).
- 26 U.S.C § 501(c)(1).
- 26 U.S.C § 501(c)(6).
- 35 U.S.C. §§ 1-376.
- 41 CRLR 515; H.R. Rep. No. 109-23, at 4 (2005), as reprinted in 2006 U.S.C.C.A.N. 1091, 1092.
- 50 U.S.C. & 401 et seq.
- 50 U.S.C. § 1801 (a)(1)-(3).
- 50 U.S.C. §1801 (k).
- 50 U.S.C. § 1802 (a)(2).
- 50 U.S.C. § 1802 (a).
- 50 U.S.C. § 1802(a)(1).

50 U.S.C. § 1809 (a).

50 U.S.C. § 1809 (c).

50 U.S.C. § 1810.

50 U.S.C. § 1810 (a)-(c).

50 U.S.C. § 1841(2).

50 U.S.C. § 1842(a)(1).

50 U.S.C. § 1861(a)(1) and (a)(2)(B).

50 U.S.C. § 1885a (a)(4).

50 U.S.C. § 1885a (a).

246 U.S. 231, 238 (1918).

522 U.S. 3, 10 (1997).

975 F.2d. at 878 (D.C. Cir. 1992).

“A Brief Introduction and History.” Library of Congress: United States Copyright Office. 14 Aug. 2009

<<http://www.copyright.gov/circs/circ1a.html>>.

“About D.A.R.E.” D.A.R.E. America. <http://www.dare.com/home/about_dare.asp>.

A Citizen's Guide on Using the Freedom of Information Act and the Privacy Act of 1974 to Request Government Records, H. Rep. No 108-372, at 15, 107th Cong., 2d Sess. (2002).

“ACLU v. NSA.” United States Court of Appeals. 14 Aug. 2009 <<http://www.ca6.uscourts.gov/opinions.pdf/07a0253p-06.pdf>>.

“An Overview of the Federal Wiretap Act, Electronic Communications Privacy Act, and State Two-Party Consent Laws of Relevance to the NebuAd System and Other Uses of Internet Traffic Content from ISPs for Behavioral Advertising.” Center for Democracy & Technology. 14 Aug. 2009 <<http://www.cdt.org/privacy/20080708ISPTraffic.pdf>>.

Federal Trade Commission and U.S. Department of Justice. Antitrust Guidelines for Competition Among Competitors. 2000. 30 Jul. 2009. <http://www.ftc.gov/os/2000/04/ftcdojguidelines.pdf>.

Aucsmith, David. Personal Interview. 14 July 2009.

Baker, Wade H., et al. “2009 Data Breach Investigations Report.” Verizon Business. 17 Aug. 2009 <http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf>.

Bazan, Elizabeth. “The Foreign Intelligence Surveillance Act: A Sketch of Selected Issues.” Congressional Research Service. p. 4. 7 Jul. 2008. 4 Aug. 2009. <<http://www.fas.org/sgp/crs/intel/RL34566.pdf>>.

Bazan, Elizabeth. Congressional Research Service. “The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and U.S. Foreign Intelligence Surveillance Court and U.S. Foreign Intelligence Surveillance Court of Review Decisions.” p. 13. 5 Feb. 2007. 4 Aug. 2009. <<http://www.fas.org/sgp/crs/intel/RL30465.pdf>> ; 50 U.S.C. § 1861(a)(1).

Brenner, Susan. Personal Interview. 03 June 2009.

Burka v. Department of Health and Human Services, 87 F.3d 508, 515 (D.C. Cir. 1996).

Critical Mass Energy Project v. Nuclear Regulatory Commission, 975 F.2d 871 (D.C. Cir. 1992).

“Center for Auto Safety v. Tiemann.” VersusLaw, Inc. 17 Aug. 2009

<http://dc.findacase.com/research/wfrmDocViewer.aspx/xq/fac.%5CFDCT%5CDDC%5C1977%5C19770225_0000034.DDC.htm/qx>.

“Collaborate.” Webster's II New Riverside University Dictionary. 1984.

“Common Challenges for Partnerships.” Partnership Guide. 29 Jun. 2009.

<<http://www.partnershipresourcecenter.org/resources/partnership-guide/chap8-3.html>>.

“Computer Security Division Computer Security Resource Center: FISMA Detailed Overview.” National Institute of Standards and Technology. 31 Jul. 2009. 14 Aug. 2009 <<http://csrc.nist.gov/groups/SMA/fisma/overview.html>>.

“Critical Infrastructure Protection.” DoD Dictionary of Military Terms. 12 Aug. 2009
<<http://www.js.pentagon.mil/doctrine/jel/DoDdict/data/c/11427.html>>.

“Critical Infrastructure Protection.” GAO Highlights. 7 Jun. 2009 <<http://www.gao.gov/highlights/d0739high.pdf>>.

Cyber Incident Annex, National Response Plan(NRP) December 2004 Cyber -1.

Cyber Incident Annex, National Response Plan(NRP) December 2004, Cyber - 6.

“Cyberspace.” DoD Dictionary of Military Terms. 12 Aug. 2009
<<http://www.js.pentagon.mil/doctrine/jel/DoDdict/data/c/10160.html>>.

“Defend.” Webster’s II New Riverside University Dictionary. 1984.

“DefenseLINK Mission.” U.S. Department of Defense. 27 Jul. 2009 <<http://www.defenselink.mil/admin/about.html>>.

Defense Security Service. International Programs: Limited Access Authorizations (LAAs) for Non-U.S. Citizens.
<<https://www.dss.mil/GW/ShowBinary/DSS/isp/international/laa.html>>. 13 Aug. 2009.

Department of the Interior v. Klamath Water Users, 532 U.S. 1, 8 (2001).

Department of Justice v. Tax Analysts, 492 U.S. 136, 144-46 (1989).

“Directive 5525.5: DoD Cooperation with Civilian Law Enforcement Officials.” Department of Defense. 12 Aug. 2009
<<http://www.dtic.mil/whs/directives/corres/pdf/552505p.pdf>>.

“Dispelling the Myths.” Department of Justice. 8 Jul. 2009 <http://www.usdoj.gov/archive/ll/subs/u_myths.htm>.

DoDD 5200.27 “Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense.

DoDD 5240.1, DoD Intelligence Activities (Apr. 25, 1998).

Doyle, Charles. “USA PATRIOT Act Sunset: A Sketch.” CRS Report for Congress. 18 Aug. 2009
<<http://www.fas.org/irp/crs/RS21704.pdf>>.

“EFF and ACLU Planning to Appeal Dismissal of Dozens of Spying Cases.” Electronic Frontier Foundation. 3 Jun. 2009. 13 Aug. 2009. <<http://www.eff.org/press/archives/2009/06/03>>.

Epsley-Jones, Katelyn and Christina Frenzel. “The Church Committee Hearings & The FISA Court.” PBS-Frontline. 15 May 2007. 12 Aug. 2009.

“Executive Order 12958 – Classified National Security Information.” The White House: Office of the Press Secretary. 12 Aug. 2009 <<http://www.fas.org/sgp/clinton/eo12958.html>>.

Executive Order 12333, para1.14(a).

Executive Order 12333, para. 3.4(a),(d) Dec. 4, 1981.

“Executive Order 13010 – Critical Infrastructure Protection.” Federal Register. 13 Aug. 2009
<<http://www.fas.org/irp/offdocs/eo13010.htm>>.

Executive Order No. 13292, Sec. 1.1(4).

“Federal Acquisitions Regulations.” Business.Gov: The Official Business Link to the U.S. Government. 19 Aug. 2009
<<http://www.business.gov/expand/government-contracting/far.html>>.

Federal Judicial History. “Foreign Intelligence Surveillance Court.” 11 Aug. 2009.
<http://www.fjc.gov/history/home.nsf/page/fisc_bdy>.

Federal Trade Commission and U.S. Department of Justice. Antitrust Guidelines for Competition Among Competitors. 2000. 30 Jul. 2009. <http://www.ftc.gov/os/2000/04/ftcdojguidelines.pdf>.

Federal Trade Commission and the U.S. Department of Justice. Guidelines for Collaboration Among Competitors. 2000.
<<http://www.ftc.gov/os/2000/04/ftcdojguidelines.pdf>>.

- Fox, Susannah and Jean Beier. "Online Banking 2006: Surfing to the Bank." The Pew Internet and American Life Project. 2006.
<http://www.pewinternet.org/~media/Files/Reports/2006/PIP_Online_Banking_2006.pdf.pdf>.
- GC Micro Corp. v. Defense Logistics Agency, 33 F.3d 1109, 1112 (9th Circ. 1994).
- Gellhorn, Ernest, William E. Kovacic, Stephen Calkins. Antitrust Law and Economics, 5th ed. Minnesota: West Publishing Co., 1994.
- General Chilton, Kevin P. 2009 Cyberspace Cymposium. 07 April 2009.
<http://www.stratcom.mil/speeches/23/2009_Cyberspace_Symposium>.
- "General Information Concerning Patents." United States Patent and Trademark Office. 14 Aug. 2009
<<http://www.uspto.gov/go/pac/doc/general/#patent>>.
- Giacomello, Giampiero. National Governments and Control of the Internet: A Digital Challenge. New York: Routledge, 2005.
- Gidiere III, P. S. (2006). *The federal information manual*. Chicago: ABA Publishing. p. 227.
- Gilmore v. Department of Energy, 4 F. Supp. 2d 912, 922 (N.D. Cal. 1998).
- Goldman, Eric. Personal Interview. 8 June 2009.
- "Hepting v. AT&T." Electronic Frontier Foundation. 13 Aug. 2009. <<http://www EFF.org/cases/hepting>>.
- Hodgkins, Trey. Personal Interview. 9 Jul. 2009.
- Holmes, William C. Antitrust Law Handbook, 2008-2009 Edition. USA: West Group, 2008.
- Homeland Security Act of 2002, Sections 212-215.
- Homeland Security Presidential Directive -7, Dec.17, 2003 (7)(a-f),2-3.
- Hosteny, Joseph N. "Litigators Corner: Patent or Trade Secret: Which one is Best?" Joseph Hosteny: Intellectual Property Attorney. 14 Aug. 2009 <<http://www.hosteny.com/archive/hosteny%2008-00.pdf>>.
- Hudson, David L., Jr. "Patriot Act." First Amendment Center. 8 Jul. 2009.
<http://www.firstamendmentcenter.org/speech/libraries/topic.aspx?topic=patriot_act>.
- Huskisson, Lt. Col. Darrin. Personal Interview. 28 June 2009.
- Kelleher, David. "Social Networking at Work: Fear Not Facebook and Myspace." February 23, 2009.
<<http://www.itworld.com/internet/63062/social-networking-work-fear-not-facebook-myspace>>.
- Kennel, John R. and Jane Lehman. "Electronic Surveillance; Wiretapping." American Jurisprudence, Second Edition. May 2009.
68 Am. Jur. 2d Searches and Seizures § 348. 13 Aug. 2009.
- Lederer, Edith M. "North Korea Sanctions Unanimously Expanded By U.N. Security Council." The Huffington Post. 7 Aug. 2009 <http://www.huffingtonpost.com////korea-sanctions-una_n_214885.html>.
- Lenhart, Amanda. "Adults and Social Network Sites." The Pew Internet and American Life Project. January 2009.
<http://www.pewinternet.org/~media/Files/Reports/2009/PIP_Adult_social_networking_data_memo_FINAL.pdf.pdf>.
- Lenich, John. Personal Interview. 01 August 2009.
- Lewis, Neil. "Patriot Act." Microsoft Encarta Online Encyclopedia 2009. 7 Jul. 2009
<http://encarta.msn.com/encyclopedia_701712693/Patriot_Act.html>.
- McDermott, Richard and Carla O'Dell. "Overcoming the 'Cultural Barriers' to Sharing Knowledge." American Productivity & Quality Center. 17 Aug. 2009.
<http://www.apqc.org/portal/apqc/ksn/Overcoming%20Cultural%20Barriers.pdf?paf_gear_id=contentgearhome&paf_dm=full&pageselect=contentitem&docid=106967>.

“Memorandum for the Heads of Executive Departments and Agencies”. 4 Mar. 2009. 10 Jul. 2009

<http://www.whitehouse.gov/the_press_office/Memorandum-for-the-Heads-of-Executive-Departments-and-Agencies-Subject-Government/>.

“Memorandum of May 27, 2009: Classified Information and Controlled Unclassified Information.” Federal Register. 17 Aug. 2009 <http://www.whitehouse.gov/the_press_office/Presidential-Memorandum-Classified-Information-and-Controlled-Unclassified-Information/>.

Miller, Arthur R., and Michael H. Davis. Intellectual Property: Patents, Trademarks, and Copyright, In a Nut Shell. Fourth Edition. St. Paul, MN: West Publishing Company, 1990.

Nagle, James F. How to Review a Federal Contract: Understanding and Researching Government Solicitations and Contracts. 2nd ed. Chicago: American Bar Association, 2000. 1.

Nakashima, Ellen and Dan Eggen. “Former CEO Says U.S. Punished Phone Firm.” *Washington Post*. 13 Oct 2007.

National Parks & Conservation Association v. Morton, 498 F.2d 765, 770 (D.C. Cir. 1974).

National Sec. Archive v. Executive Office of the President, 688 F. Supp. 29 (D.D.C. 1988), aff’d 909 F.2d 541 (D.C. Cir. 1990).

National Strategy for Homeland Security, Office of Homeland Security, Jul. 2002.

Olson-Jones, Tiffany. Personal Interview. 15 June 2009.

President Barack H. Obama, “Memorandum of May 27, 2009—Classified Information and Controlled Unclassified Information,” p. 26277.

“Private Sector.” DoD Dictionary of Military Terms. 12 Aug. 2009.

<<http://www.js.pentagon.mil/doctrine/jel/DoDdict/data/p/19545.html>>.

Professor Bill Lyons, Nebraska College of Law. Personal interview, July 27, 2009.

“Protection.” DoD Dictionary of Military Terms. 12 Aug. 2009

<<http://www.js.pentagon.mil/doctrine/jel/DoDdict/data/p/10741.html>>.

Public Law 107-296, 6 U.S.C. 101 note.

Risen, James and Eric Lichtblau. “Bush Lets U.S. Spy on Callers Without Courts.” *New York Times*. 16 Dec. 2005. 13 Aug. 2009.

<<http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=1&ei=5089&en=e32070e08c623ac1&ex=1292389200>>.

Ryan, Daniel. Personal Interview. 16 Jun. 2009.

S. Bill 876. The Library of Congress. Introduced by Senator Arlen Specter. 23 Apr. 2009. 13 Aug. 2009.

<<http://thomas.loc.gov/cgi-bin/bdquery/D?d111:1:/temp/~bdyjyp:@@L&summ2=m&/bss/111search.html>>.

Schlansker, Bob. Personal Interview. 15 Jun. 2009.

“Securing Cyberspace for the 44th Presidency.” 23Dec. 2008,

Security Classification Policy and Procedure: E.O. 12958, as Amended. Congressional Research Service.

“Smart Card Alliance Government Conference Opens with DoD Network Security Case Study.” Government Technology: Solutions for State and Local Government in the Information Age. 19 Jun. 2009

<<http://www.govtech.com/gt/articles/104934>>.

Smith, Stephanie. “Federal Advisory Committees: A Primer.” CRS Report for Congress. 14 June 2009.

<<http://www.fas.org/sgp/crs/misc/RL30260.pdf>>.

Sullivan, Bob. “‘La Difference’ is Stark in EU, U.S. Privacy Laws: EU Citizens Well-Protected against Corporate Intrusion, but Red Tape is Thick.” 10 Aug. 2009 <<http://www.msnbc.msn.com/>>.

“The Clinton Administration’s Policy on Critical Infrastructure Protection: Presidential Decision Directive 63.” Presidential Decision Directives. 17 Aug. 2009 <<http://fas.org/irp/offdocs/paper598.htm>>.

- “The D.A.R.E. Mission.” D.A.R.E. America. <www.dare.com/home/THEDAREMISSION.asp>.
- “The Federal Advisory Committee Act.” Federal Open Government Guide. 16 Jul. 2009
<<http://www.rcfp.org/fogg/index.php?i=faca>>.
- “The Patriot Act and the First Amendment: A Statement from the Freedom to Read Committee of the Association of American Publishers.” 17 Aug. 2009 <<http://www.publishers.org/main/AboutAAP/attachments/patriotact.pdf>>.
- “The PATRIOT Act’s Impact on your Rights.” American Civil Liberties Union. 14 Aug. 2009
<<http://www.aclu.org/PatriotActFlash/PatriotActFeature.htm>>.
- “The President’s National Security Telecommunications Advisory Committee: Executive Summary.” NSTAC XXV Issue Review: 20th Anniversary Edition 1982-2002. (2002): 123 as cited in Westby, Jody R., Ed. International Guide to Cyber Security. Chicago: ABA, 2004.
- Tien, Lee and Peter Eckersley. “A Letter to the White House Cyber Security Review Team.” *Electronic Frontier Foundation*. (undated).
- Tien, Lee and Peter Eckersley. “Letter to the Administration.” *Electronic Frontier Foundation*. (undated)
- Title 5 § 107(a)(2).
- Title 5 § 552(b)(5).
- Title 5 § 552(b)(6).
- Title 5 § 552(b)(7).
- Title 5 § 552(b)(8).
- Title 5 § 552(b)(9).
- Title 10 § 130.
- Topoliski, Robb. Personal Interview. 15 Jun. 2009.
- “Trade Secret.” Black’s Law Dictionary. 8th ed. 2004.
- “Trade Secrets v. Patents.” Invention Resource International. 14 Aug. 2009
<http://www.inventionresource.com/index.php?option=com_content&view=article&id=37>.
- “Twenty-Seventh Annual Report of the President on Federal Advisory Committees.” Federal Interagency Databases Online. 13 Aug. 2009 <<http://fido.gov/facadatabase/printedannualreports/1998-Twenty-Seventh%20Annual%20Report%20Of%20The%20President%20On%20Federal%20Advisory%20Committees.pdf>>.
- Uniform Trade Secrets Act of 1979 § 1(4), 14 U.L.A. 542 (1979).
- “United States Extradition Treaties.” Nation Master. 10 Aug. 2009 <http://www.nationmaster.com/_uni_sta_ext_tre_cit-united-states-extradition-treaties-citation>.
- U.S. Const. amend. I.
- U.S. Const. amend. IV.
- U.S. Courts. “Understanding Intelligence Surveillance: A FISA Primer.”
<<http://www.uscourts.gov/outreach/topics/fisa/whatisfisa.html>>.
- Vine, David. “Look After the Pennies.” *Working Life*. Apr. 2009. <www.AccountancyMagazine.com>.
- Weeks, Jeffery. Personal Interview. 02 July 2009.
- “When is Federal Advisory Committee Act (FACA) Applicable?” U.S. General Services Administration. 29 Jul. 2009
<http://gsa.gov/Portal/gsa/ep/contentView.do?contentType=GSA_BASIC&contentId=10348>.
- Wybourne, Martin N., Martha F. Austin, and Charles C. Palmer. “National Cyber Security Research and Development Challenges Related to Economics, Physical Infrastructure, and Human Behavior.” *An Industry, Academic, and Government Perspective*. Institute for Information Infrastructure Protection (I3P), 2009.

Yen, Alfred C. and Joseph P. Liu. "A Brief Introduction and History." Copyright Law: Essential Cases and Materials. St. Paul, MN: Thomas/West, 2008.

APPENDIX 1: OUTREACH CONTRIBUTORS

Scott Algeier – Founder, President and CEO Conrad, Inc.; Executive Director of the Information Technology- Information-sharing and Analysis Center (IT-ISAC)

Professor Marvin Ammori – University of Nebraska College of Law

Mark Atalla – Chief Technology Officer, Center for Advanced Defense Studies

David Aucsmith – Senior Director, Institute for Advanced Technology, Microsoft

Stewart Baker – Partner- Steptoe & Johnson, LLP

Maj. Heather Blackwell –Legislative Fellow, Office of Sen. Ben Nelson

Professor Susan Brenner – Professor of Law, University of Dayton School of Law

Jeff Brown – Director, Infrastructure Services and Chief Information Security , Raytheon

Matt Churchill – Director, Digital Forensics and Cyber Investigation, Continuum Worldwide

Robert Corn-Revere – Partner--Davis, Wright, Tremaine, LLP

Ian Crone – Researcher, Center for Advanced Defense Studies

Jim Dempsey – Vice President for Public Policy, Center for Democracy and Technology

Professor Maeve Dion – Legal Research Associate, Critical Infrastructure Protection Program, George Mason University School of Law

June Edwards – Principal, Constellation Consulting

Eric Fisher – Senior Specialist in Science and Technology Resource, Science and Industry Division Congressional Research Service

Gregory Garcia – Founder Garcia Strategies, LLC

Rob Georgi – Special Agent, Federal Bureau of Investigation

Darrin Gilchrist – Staff Judge Advocate, Joint Task Force-Global Network Operations

Wendy Ginsberg – Analyst in American National Government, Government and Finance, Congressional Research Service

Professor Eric Goldman – Associate Professor, Director of the High Tech Law Institute, Santa Clara University School of Law

Roger Halbheer –Chief Security Advisor Europe, Middle East & Africa, Microsoft

John Havermann II – NCSA Board of Directors; Vice President, Cyber Programs, Director, Advanced Information Assurance Programs, Chief Systems Engineer, SAIC

J. Michael Hickey – Vice President, Government Affairs, National Security Policy, Verizon Communications, Inc.

Trey Hodgkins – Vice President for National Security Procurement and Policy, Tech America

Rick Holmes – Vice President, Production Systems, Union Pacific

Robert Housman – Acting Executive Director and Chairman of the Board, Cyber Secure Institute

Lt. Col. Darren Huskisson -- USAF, Chief, Operations Law Joint Task Force – National Capital Region

Stephanie Johanns – Senior Vice President, Federal Government Affairs, Verizon Communications, Inc.

Shannon Kellogg – Director of Information Security Policy, Office of Government Relations, EMC Corp

Professor John Lenich – University of Nebraska College of Law

Professor Brian Lepard – University of Nebraska College of Law

Dr. Jeremy Lipschultz – Professor and Director of School of Communications, University of Nebraska- Omaha

Professor Richard Loeb – University of Baltimore College of Law

Dr. Catherine Lotrionte – Adjunct Professor of Law; Associate Director, Institute for International Law and Politics, Georgetown University

Professor Bill Lyons – University Nebraska College of Law

Steve Naplan – Vice President for National Security, Business Executives for National Security

Professor Steve Nugen – Peter Kiewit Institute, University of Nebraska- Omaha

Jacob Olcott – Staff Director of the Subcommittee on Emerging Threats, Cybersecurity, Science and Technology, U.S. House of Representatives

Tiffany O. Jones – NCSA President; Director, Government Relations, Americas, Symantec Corporation

Dr. Steven Rinaldi – Manager, Effects-Based Studies Department, Sandia National Laboratory

Professor Daniel Ryan – National Defense University

Bob Schlansker -- ISSA Chapter President; Chief Information Assurance Engineer, ARTEL, Inc.

Paul Schuh – Associate, Booz Alan Hamilton

Andrew Serwin – Partner- Foley & Lardner, LLC

Steve Shirley – Executive Director, Department of Defense Cybercrimes

Nicki Sitler – Contract Administrator, Northrop Grumman Corp.

Jay Stanley – Director of Public Education, Liberty Program, American Civil Liberties Union

Catherine Theohary – Analyst in National Security Policy and Information Operations, Foreign Affairs, Defense and Trade Division, Congressional Research Service

John Tokar – National Security Agency

Robb Topolski – North America Foundation; Chief Technologist, Open Technology Initiative

Professor Frans von der Dunk -- University of Nebraska College of Law

Jeffery Weeks – Vice President and CISO, Jeffery Consulting & Provident Bank

Jody Westby – CyLab Distinguished Fellow, Carnegie Mellon; CEO, Global Cyber Risk, LLC

Dr. Jonathan Zittrain – Professor of Law, Harvard University

APPENDIX 2: ABOUT THE AUTHORS

Frederick Bartell received his Bachelor of Arts degree in Psychology from the University of Nebraska-Lincoln in 2006. Following graduation, he spent one year as a full-time volunteer with the Americorps VISTA program working for the EdLaw Project in Roxbury, Massachusetts. After completion of his term of service, Fritz enrolled at the Nebraska College of Law where he is currently a third-year law student. Fritz's academic interests include constitutional law, intellectual property, and government policy and regulation issues.

Aaron Brugman is a Cadet First Class at the United States Air Force Academy in Colorado Springs, Colorado majoring in Systems Engineering Management. After graduation, he will attend pilot training in Florida.

Carrie Lacy is an active member of the University of Nebraska-Omaha Sociology/Anthropology Department as a second-year graduate student. She currently serves as the Graduate Student Representative to the faculty, President of the Student Anthropological Society, and Assistant to the Alpha Kappa Delta Alpha-Chapter Advisors. Her current research focuses on the Epigenetics of Disease, Environmental Conservation, Social Movements, and Tuberculosis. Carrie recently took 2nd place at the Nebraska Undergraduate Sociological Symposium for her work on curing Tuberculosis in South Asia. Her academic and career goals involve conducting research and proposing strategies to aid in curing contagious diseases and preserving environmental resources.

Melissa Moraczewski is a senior at the University of Nebraska-Lincoln and is finishing her Bachelor of Science degree in International Business with minors in Spanish and Accounting. She grew up in Gretna, Nebraska where she attended high school and graduated as Valedictorian. She has recently completed study abroad trips in San José, Costa Rica, and Sevilla, Spain to practice Spanish and volunteer as an English teacher. She plans to attend graduate school, continue traveling, as well as begin learning new languages.

Tanya Nodlinski will be starting her final year of law school in the fall at the University of Nebraska College of Law. Before law school, she worked as a legislative staffer for Senator Tom Baker and Senator Bill Avery at the Nebraska State Legislature and also taught English for a year in South Korea at a boys' high school. She grew up on a farm outside of Grant, Nebraska and graduated with a Bachelor of Science in Political Science and an English minor from Nebraska Wesleyan University.

Sarah Norris graduated summa cum laude from Creighton University in the spring of 2009. In the fall of 2009, she will begin a joint degree graduate program at the University of Nebraska-Lincoln pursuing a Ph.D. in Clinical Psychology as well as a Master of Legal Studies.

Kate Prasse is a third-year law student at Creighton University. She was born and raised in Milwaukee, Wisconsin. Prior to attending law school, Kate received her Bachelor of Arts degree in Journalism magna cum laude from Creighton. Currently, Kate is a member of the Creighton Law Review and serves as Student Articles Editor.

Ashley Thomalla graduated from the University of Nebraska-Lincoln in the fall of 2006 with a Bachelor of Arts degree in Psychology and a minor in Sociology. In August of 2007, she started graduate school at the University of Nebraska-Omaha where she is currently a third-year M.A./Ph.D. student in the Industrial/Organizational Psychology program.

Kate Zielinski received a Bachelor of Science in Business Administration magna cum laude from the University of Nebraska-Omaha in 2007 with a specialization in Economics and a minor in Political Science. While at UNO Kate was active in student groups, held a part time job, and interned for Congressman Lee Terry in Washington, D.C. Kate will graduate in 2010 from the University of Nebraska College of Law with an emphasis in Business Transactions. Kate clerked for the Lancaster County District Court and has been involved in various student groups.